



The Leader in e-Safety Education



I-SAFE CURRICULUM SAMPLES

REV#5.2



i-SAFE Curriculum Samples



Duplication and/or selling of the information contained within this document, or any other form of unauthorized use of this copyrighted material, is against the law and a punishable crime. © 2008 i-SAFE Inc.



Dear Educators,

i-SAFE offers an innovative, student-centered curriculum for grades K-12 by integrating best practices in teaching and learning with opportunities for youth empowerment and outreach. Each lesson is designed to foster active participation between students and their instructors as learners age-appropriately build an understanding of Cyberspace as a community with real-world consequences. Integral to each lesson is the incorporation of an age-appropriate empowerment activity to provide students with opportunities to share what they have learned about Internet safety with their peers, their families, and the community. In this way, students internalize and take ownership of the concepts learned. i-SAFE curriculum is only available to educators who have completed the i-SAFE Professional Development Program (PDP) through a live workshop or online at <http://ilearn.isafe.org>.

All i-SAFE lessons are aligned with the National Educational Technology Standards for Students (NETS), individual state educational technology standards, National Media Literacy Standards, and the National Health Education Standards. The activity-based format also enables the materials to be aligned with content standards and benchmarks in the areas of Social Studies, Civics, Career and Life Skills, Health and Safety, Political Science/Civics, and Language Arts.

I have prepared this lesson plan sampler for your review as a resource in planning for i-SAFE implementation in your schools. In addition to lesson plans, the complete curriculum provides a variety of resources including the activity-format workbooks, HTML activities, songs on audio CD for young children, video webcasts, PowerPoint presentations, and regularly updated educator resources. Suggested grade levels are provided in each lesson plan. Educators are encouraged to choose lessons appropriate to the knowledge and experiential levels of their students. This booklet includes a sampling of the more than 200 lessons and activity selections available.

For the Elementary Grades:

- Music/Movement sample activity plan: "I Got a Buddy" (Gr. K-3)
- Cyber Citizens in the Cyber Community (Gr. 1)
- E-mail safety Basics (Gr. 1-3)
- Excerpt from the IN SYNC with Internet Safety workbook (Gr. 3-4)
- Excerpt from Intellectual Property UNIT: Overview and Lesson 1 (Gr. 4)
- Text messaging Safety (Gr. 5)

For the Middle Grades:

- Excerpt form Personal Safety UNIT: Overview and Lesson 2 (Gr. 6)
- Excerpt form Cyber Security UNIT: Overview and Lessons 1 & 2 (Gr. 7)
- Cyber Bullying (Gr. 8)
- Willing Participant (Gr. 7-8)
- Excerpt from the iCREATM Middle School UNIT: Intellectual Property and Copyright
- Negative Networking: A Look at Gangs Online (all middle grades)

For the High School Grades:

- A Web 2.0 World (Gr. 6-12)
- Online Social Networking
- Legal Trends in Cyber Safety and Security
- Learn Before You Burn
- Video Webcast Lesson Plan: Cyber Relationships
- Excerpt from the Internet Life Skills Series 2 Workbook
- Service Learning: i-Adopt-A-School

I hope you enjoy the curriculum materials. Please do not hesitate to contact me directly with any questions about curriculum or i-SAFE implementation planning. Thank you for your interest in i-SAFE!

Sincerely,

Carolyn Walpole

Carolyn E. Walpole
Director of Curriculum Development
i-SAFE Inc.
cwalpole@isafe.org

Music & Movement Sample: I Got A Buddy

Activity Goal

Learners will have fun making i-Buddy puppets and using them to “dance” to the music while reviewing how to make good decisions when online. Students will:

- Understand that i-Buddy is their friend to help them make wise choices online
- Review good decisions to make when going online
- Be able to list some of the bad decisions they can make when going online

Materials / Preparation

- Keyboard or other means to play the song
- Optional: media player and a copy of the song in MP3 format from the Curriculum CD or audio CD recording from the sing with i-Buddy CD, available for purchase at <http://auth.isafe.org/store/>

ACTIVITY PLAN

- Inform students that you are going to play them a song about i-Buddy. During the song they are to think about what lessons i-Buddy has taught them. After the song you will be asking for their feedback on what they remember from the i-SAFE lessons.
- Play *I Got A Buddy* for students.
- Discussion:
 - Ask students who the buddy is that is mentioned in the song? *i-Buddy*
 - What are some things i-Buddy has taught us about going online? *Asking for help, viruses, strangers, etc.*
 - What are some good decisions we can make when we go online? *Ask for help, get out of bad sites, don't open email from strangers, etc.*
 - Why do we need to stay safe online? What kinds of dangers are there? *Viruses, people you don't know, unsafe places.*
 - Correct. As we learned in our i-SAFE lessons there are three main dangers we need to be aware of: Viruses, people you don't know, and unsafe places. While on the Internet we can click on items or open emails that contain viruses. These can make our computer very sick. We wouldn't want that. Another danger on the Internet is to come across people you don't know. We have to be very careful about STRANGERS online. Sometimes they want to hurt us. Finally we need to be aware of unsafe places. While on the Internet we can sometimes be surprised with items we don't want to see or shouldn't see. Adults can help us navigate safely so we aren't surprised with bad things.
- What are some bad decisions we can make when we go online? *(Not getting help, going to places we know are bad, downloading things without permission, etc.)*
- Hand out the i-Buddy paper activity sheet.
- Allow students time to make their i-Buddy puppet while listening to the song.

Alternative Activity Suggestions

- Have students draw pictures while the song is playing of what it means to them. Share the songs with the class and discuss what they know about safety online.
- Have students come up with a “second friend” to go with i-Buddy that will help them also remember Internet safety rules.

I Got A Buddy Lyrics

I Got a Buddy (Written by Benny C. Uyetake)

I got a Buddy
Who will help me with
The tools of the Internet. (4x)

I got a buddy
Who will keep me safe
Working on the Internet (4x)

I got a buddy
Who will help me make
Right choices on the Internet (4x)

I got a buddy
Who will help me be
Responsible on the Internet (4x)

I got a Buddy
And you got a Buddy
Surfing on the Internet

I-Buddy,
I-Buddy is the best
Surfer on the Internet (optional lyrics)

(chorus)
He's named I-BUDDY
Surfer on the cyber space highway
I-BUDDY
He's my buddy while I'm on-line

I Got a Buddy

Benny C. Uyetake

$\bullet = 76$

The musical score is written on a single staff in treble clef with a common time signature (C). The tempo is marked as 76 beats per minute. The key signature is C major. The score consists of 12 measures. Chords are indicated by letters above the staff: C, G7, F, and C. The lyrics are written below the staff, with some words split across lines. The score ends with a double bar line and repeat dots.

I got a bud-dy who will help me with the tools of the In - ter - net

I got a bud - dy who will help me with

tools of the In - ter - net I got a bu - dy that will help me with

I got a bud-dy who will help me with I got a bud-dy who will help me

with the tools of the In'ter - net his name is I - Bud - dy

surf - er on the cy - ber space high - way I - Bud - dy he's my

bud - dy while - I'm online

Additional lyrics

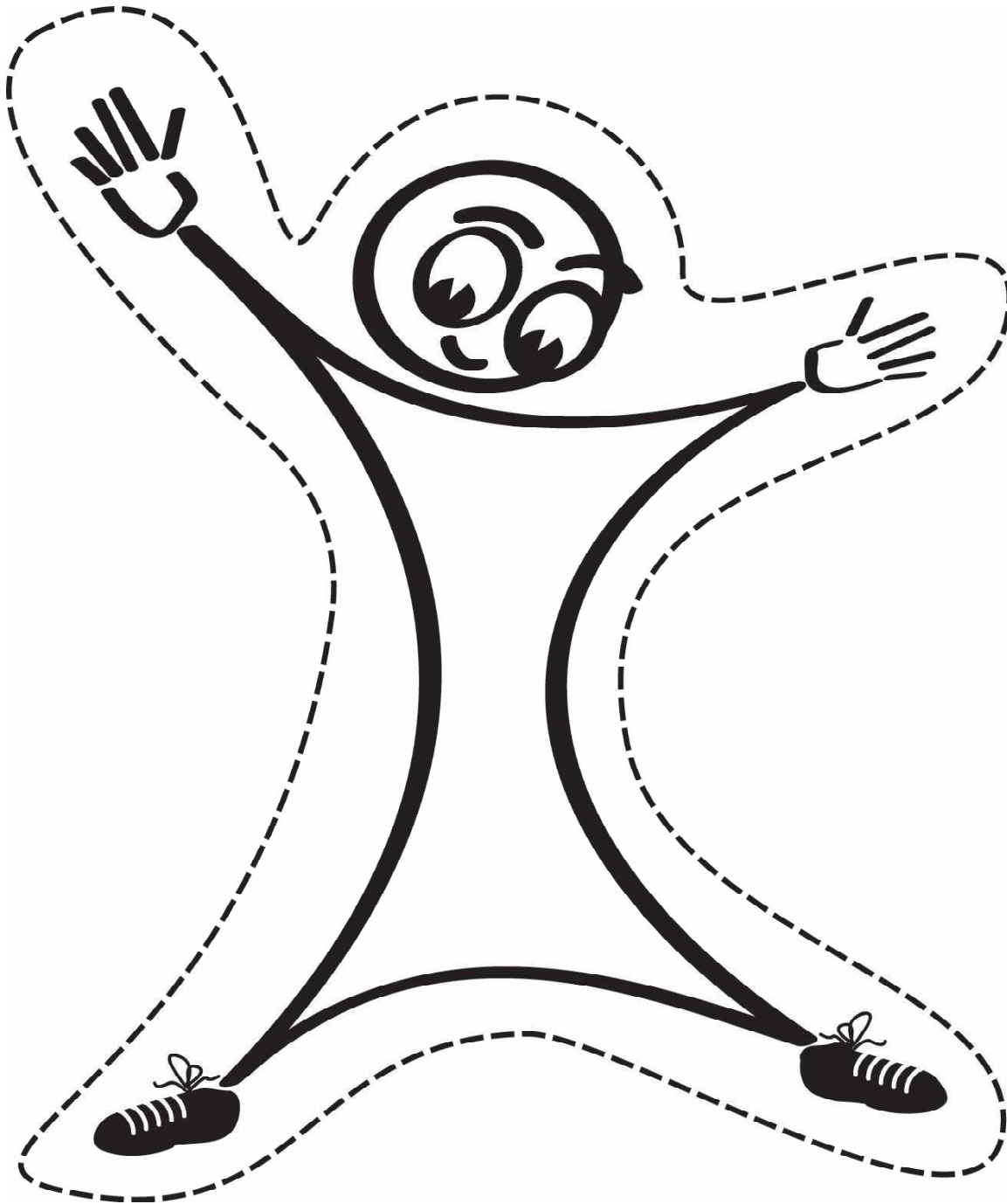
I got a buddy who will keep me safe
working on the Internet 4x

I got a buddy who will help me make
Right choices on the Internet 4x

I got a buddy and you got a buddy
Surfing on the Internet 4x

i-Buddy puppet

Directions: color, cut on dotted line, and glue or tape to a craft stick, straw, or paper bag.



CYBER CITIZENS in the CYBER COMMUNITY

i-SAFE Lesson Plan

Suggested Grade Level 1

Goal

Learners will develop an understanding of the concept of community and apply it to knowledge of the Internet. Students will engage in a group discussion moderated by the teacher, to gain a basic understanding of a comparison of the physical community to the abstract concept of Cyberspace as a community. Throughout the lesson, students will complete activities in an activity mini-booklet to express their ideas and reinforce concepts introduced.

Note: In the early elementary grades it is suggested that the lesson on Cyber Community Citizenship be completed before any other i-SAFE lessons.

Materials / Preparation

A copy of the mini-booklet (pre-folded), markers, or pencil for each student

Youth Empowerment

This learning unit will incorporate the core lesson activities into a correlated empowerment activity. Learners and instructors will choose a Youth Empowerment activity which best reflects their needs and interests.

Assessment (Grades K – 2)

Assessment should be completed after implementation of the last i-SAFE lesson.

In ilearn downloadable materials and in print versions of the curriculum, assessment instructions and student pages are located at the end of the lesson on personal safety. These materials are also found in the “Downloads” section of the i-SAFE K-5 Curriculum CD.

LESSON OUTLINE

Introduce Internet Safety

Option: Play a selection from the songs located in the “Downloads” section of the K-5 curriculum CD or on the Sing with i-Buddy audio CD, available for purchase at <http://auth.isafe.org/store>.

- Provide students with a mini-booklet and have them write their names in the space provided. Tell them that they will do activities in the mini-booklet during this lesson.
- Introduce the i-SAFE character, “i-Buddy”. *Activity booklet: Cover*

Compare the physical community to the cyber community by providing open-ended questions to prompt discussion. Use the mini-booklet as a guide, and have students complete the pages as you go along. Include the following:

1. What is a community? *(The area where we live, which contains places where we know real people.) Activity booklet: Page 1*
2. How do we get from place to place in our community? *(1) Walking, types of vehicles and types of roadways etc. (2) With assistance from trusted adults.*
3. What does the word Cyberspace mean? *(A community, which contains places to visit, just like in the real community. It is called the cyber community. Places in the cyber community are called websites.) Activity booklet: Page 2*
4. How do people get around in the Cyberspace? *(1) By using the Internet. (2) With adult assistance. Activity booklet: Page 3*
5. Can you get lost in Cyberspace? *(Yes.) Activity booklet: Pages 4 and 5*
6. What should you do if you get lost in Cyberspace? *(Get help from a grown up.)*
7. What is a citizen? *(A member of a community.)*
8. What do we call citizens in Cyberspace? *(Cyber citizens.)*
9. Identify people who help us follow rules? *(Law enforcement officers, parents, coaches, teachers, etc.)*
10. Identify the similarity between community rules and laws and Cyberspace rules. *(Include: Parents as the primary educators – they make rules to keep their children safe.)*
11. Have students tell how they can be good cyber citizens. *Activity booklet: Page 6*
12. Reinforce that i-Buddy wants kids to follow the rules that their parents or guardians make for them concerning computer and Internet use. i-Buddy says if they do, that’s being Cyber Smart, and Cyber Smart is Cyber Safe!

Review the lesson by asking and reviewing the answers the following questions:

1. “How is Cyberspace a kind of community?”
2. “Who can tell me a good place or website to visit in Cyberspace?”
3. “What should you do if you accidentally end up in the wrong place?”
4. “How can you be a good citizen in Cyberspace?”

Culminating Activity

Give the students time to finish coloring the activity booklets.

Empowerment in Action

Select a student empowerment activity. You may select one from the end of the lesson plan or use your own Outreach idea:

LESSON PLAN with EXAMPLE DIALOGUE

Provide students with a mini-booklet and have him or her write their names in the space provided. Tell them that they will do activities in the mini-booklet during this lesson.

Introduce internet safety

Option: *Play a selection from the songs located in the "Downloads" section of the K-5 curriculum CD or on the Sing with i-Buddy audio CD, available for purchase at <http://auth.isafe.org/store>.*

"Take a look at your booklets. The cover says 'i-SAFE', and has a picture of a character named i-Buddy on it. There's a place for you to write your name, so write your names on your booklets now."

"The character on the cover of your booklets is i-Buddy. For a few days, i-Buddy is going to help us with activities to learn about Internet safety. Today, he is going to help you learn about the community called Cyberspace, and what it means to be a good cyber citizen. We are also going to discuss some great places to go in Cyberspace, and what to do if you go somewhere you don't mean to. We are going to learn and use words that some of you may not know, so be sure to tell me if you don't understand a word that I use."

Question: "Who can tell me what a community is?" *Provide time for student responses.*

"Open your booklets and take a look at the first page. What are some of the pictures that you see?" *Provide time for student responses.*

"These are all places that make up our community or neighborhood. These are places where we know real people."

Question: "How do we get from place to place in our communities?"
Provide time for student responses. (*Answers should include walking, types of vehicles, and types of roadways: streets, roads, highways, and freeways*).

"Let's take a little time to draw in some roads and ways to travel on this page. You can color it in more completely later if you want to." Provide a few minutes, and then have the students share what they have drawn with the group.

Question: "Okay, let's go on. Can anyone tell me what the word Cyberspace means?"

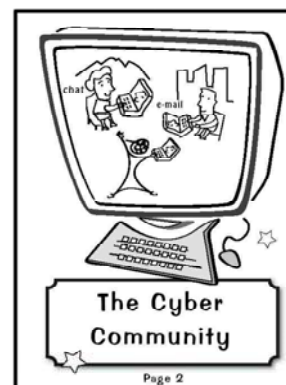
Provide time for student responses. (Answers will vary.)

Question: "Do you know that Cyberspace is a community just like the one we live in?"

Provide time for student responses.

"Let's find out more about Cyberspace. Turn to page 2 in your booklets. What do you see? Right! There are libraries, stores, museums, and all kinds of cool places in Cyberspace for learning and for having fun. We call it the Cyber community. Look at i-Buddy. He's got a happy face to show that he thinks Cyberspace is fun. You can visit places in the Cyber community just like you can visit them in the community or neighborhood where you live. Places in the Cyber community have a special name; does anyone know what they are called?" *Provide time for responses.*
"Yes, we call them Websites."

Question: "But how do we get to Cyberspace? Are there roads to the websites?" *Provide time for student responses.*

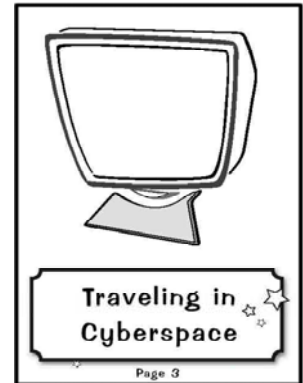


"Right, you get there with a computer instead of by walking or by car or bus. It's easy to visit places in Cyberspace because you don't have to leave your home, and most places are open all the time. "The road to the Cyber community is called the Internet. Sometimes it's called a Superhighway, and just like when an adult drives you around on a real highway, kids need an adult to help them get around on the Internet superhighway."

Note: Gauge the following part of the lesson to your students' Internet experience level.

Question: "How many of you have been on the Internet?" *Provide time for student responses.*

"Wow, some of you know a lot about the Internet! Take a look at page 3 in your activity booklets. Let's take some time to draw or write your ideas of what you can use to go places in Cyberspace." *(Students will draw a variety of things: lines, a mouse, www, etc., depending on the level of Internet experience. If necessary, provide hints and help for those who can't think of something).*



Question: "How many of you have been to websites with your parents, older brothers or sisters, or with a teacher here at school? Let's go around the class and have each person think of a good website they have visited. If you haven't been to a website yet, imagine a place you think you'd like to go to." *Provide time for student responses.*

"Those sound like great places! I'd like to visit them too!" *(Add examples if necessary).*

"If you haven't been on the Internet yet, you probably will before too long, so it's important for you to know about it."

"Listen to what happened to i-Buddy when he was on the Internet. One day i-Buddy's dad helped him get to a fun website to play a game. While he was there, i-Buddy clicked the mouse a few times and ended up in a different place. He couldn't read what it said, but he knew it wasn't where he wanted to be. He tried to go back to the game, but he couldn't."

Question: "How do you think i-Buddy felt when he got lost?"

Provide time for student responses. (He was worried)

"This is how the story turned out: i-Buddy called for help. His dad came in and helped him get back to the right place really fast. Do you think his dad was mad at him?" *Provide time for student responses.*

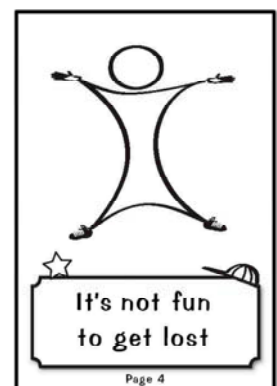
"Do you have an idea of what his dad told him? His dad said if he ever ended up in the wrong place again he should just stop, and find a grown-up to help him get back. He wasn't mad at all! It wasn't i-Buddy's fault; anyone can get lost on the Internet, even adults!"

Question: "Let's make a rule. Can you think of a rule for being in Cyberspace that we can create from hearing about i-Buddy's experience?" *Provide time for student responses. (Create a rule about getting an adult's help if you get lost in Cyberspace.)*

"This is a good rule! If you get lost in Cyberspace, call an adult right away for help."

"Turn to the next page (page 4) in your booklet."

"Let's read it. It says, 'It's not fun to get lost'. We just learned that you could get lost when you are on the Internet. It's like taking a wrong turn on a real road. You can get to a website that you don't mean to get to, and then not know how to go back. Draw in i-Buddy's face to show how he felt when he was lost on the Internet, and draw an adult you would call."



“On the next page (page 5), draw in i-Buddy’s face to show how he felt when he got help, and draw an adult you would call. Let’s read that page together: Call an adult for help.”

Question: “i-Buddy’s experience of getting lost on the Internet seems a lot like getting lost in the real community, doesn’t it?”

Question: What’s a good rule to follow if you get lost in your neighborhood community?” Provide time for student responses, and answer appropriately. (*Find a trusted adult: someone who works in a store, policeman, etc., and tell them you are lost.*)



Question (review): “Tell me again - what should you do if you get lost in Cyberspace?” (Get help from an adult.) Provide time for student responses.

Question: Do you think i-Buddy could get lost again?” Provide time for student responses. “I think he can get lost again, but now he knows what to do.”

Review rule: “What should you do if you get lost in Cyberspace? Right! Follow the rule you made: stop and find a grown-up to help.”

Activity: “Let’s practice ways to ask for help if you get lost on the Internet. Do you think you should just yell and scream at the top of your lungs? No, of course not; tell me some ways you could ask for help nicely.” *Provide time for student responses.* “Now that you’ve heard about i-Buddy’s story, let’s talk about how we stay safe in our communities.”

Present the idea: “Following good rules in the real community and the cyber communities keep us safe.”

Question: “Does anyone know what a citizen is? *Provide time for student responses.* “A citizen is someone who is part of a community.”

Question: “Are you a citizen in a community?” (Yes!)

Present the idea: “When you follow good rules in the real community and the cyber community, we say you are being a good citizen.”

Question: “Can you think of a good name for a citizen in the cyber community? Provide time for student responses. “Cyber citizen is a good name! When you are in Cyberspace, you are a cyber citizen!”

Question: “If you are a good citizen, who makes up good rules to keep you safe?” Provide time for student responses.

Present the idea: “For you, most of the rules you follow are made by your parents and your teachers. Parents protect their children by making rules for them to follow when they are out in the community.”

Question: “What are some of the rules that your parents have made?” Provide time for students to respond. (Answers should include don’t talk to strangers, tell your parents where you are going, wear your seatbelt, look both ways when you cross the street, etc.)

“Why do parents think their children need rules?” (*To keep them safe.*)

“Let’s review what we have talked about.”

“We have learned that:

- Rules are made to keep people safe.

- Parents keep their children safe by making rules for them to follow when they are out in the community.
- When you follow the rules of your community, you are a good citizen.
- When you follow the rules in the cyber community, you are a good cyber citizen."
-

Question: "Look at page 6 in your booklet. Can you read it? Right! It says, 'I am a good citizen.' Draw a picture of yourself in the space next to i-Buddy." *(When finished, have everyone "read" the sentence together)*

Question: "Do you think i-Buddy was being a good cyber citizen when he called for his dad's help?" Provide time for student responses."

"i-Buddy wants you to remember that kids should follow the rules that their parents or guardians make for them concerning computer and Internet use. i-Buddy says that is being Cyber Smart, and Cyber Smart is Cyber Safe!"



Review

"I think you know a lot about visiting the cyber community. Can you help me remember some of the things you learned today? I think you can! I'm going to ask you some questions now. Help me remember the answers."

"How is Cyberspace a kind of community?"

"Who can tell me a good place or website to visit in Cyberspace?" Repeat the answers back to the class.

"What should you do if you accidentally end up in the wrong place?"

"How can you be a good cyber citizen in Cyberspace?"

Culminating Activity

Give the students time to finish coloring the activity booklets.

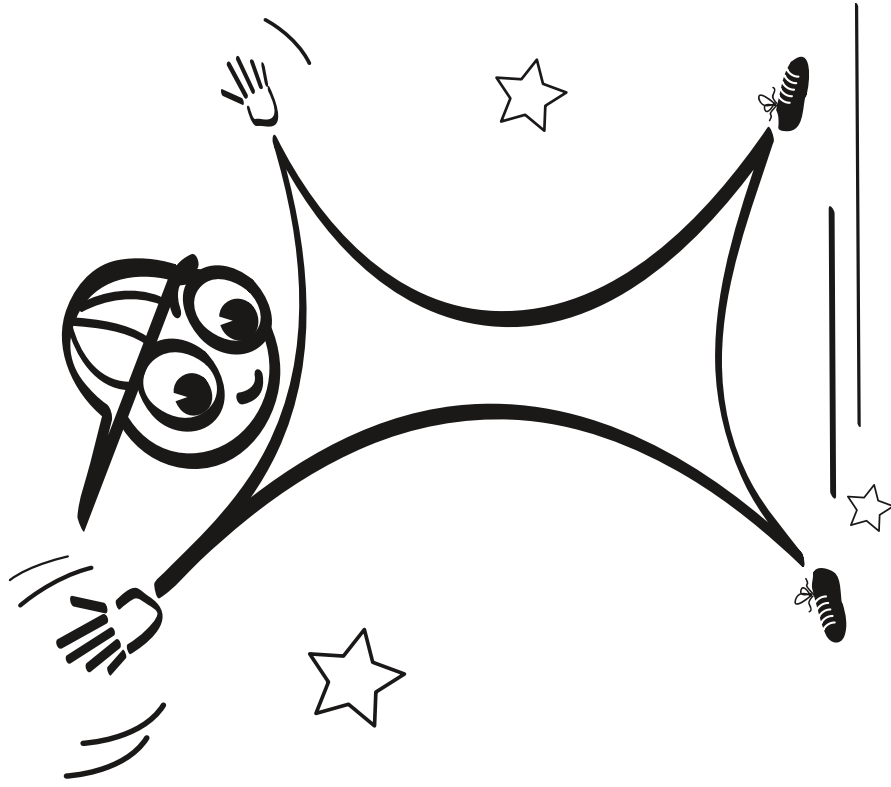
Empowerment in Action

Select one of the following to incorporate Youth Empowerment and Outreach:

- Have the students take their booklets home and tell their parents everything they learned about Internet safety today.
- Have the students create a poster about being a good citizen in Cyberspace.
- Using age appropriate software, have the students make a picture about good citizenship on the Internet, and display it in the computer lab or media center.
- Have the students write a short i-Buddy story about good cyber citizenship and share them with another class.

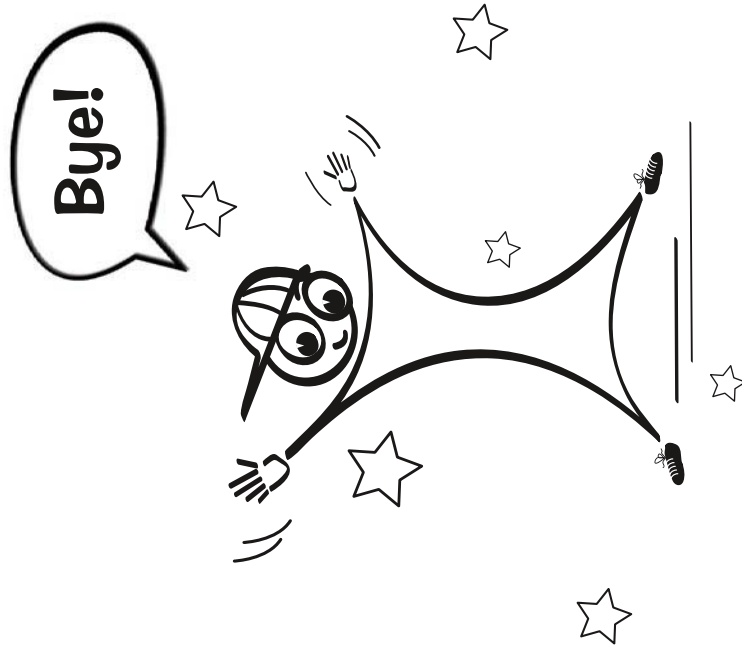
Conclusion

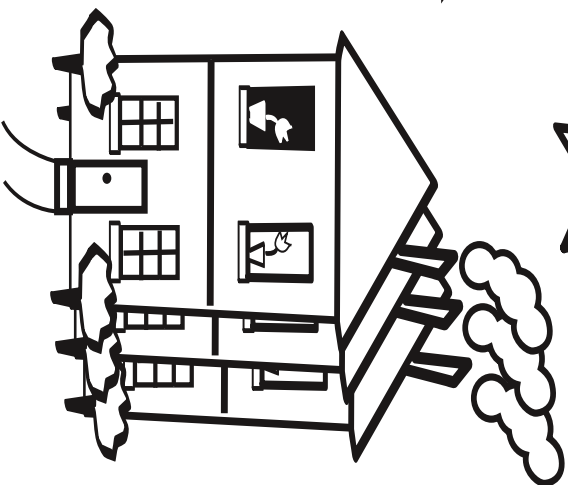
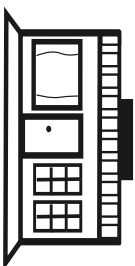
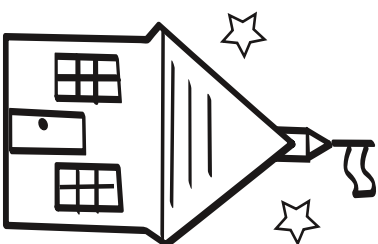
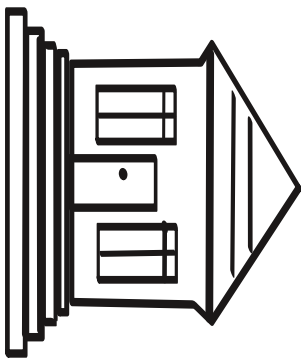
- Complete the Assessment activity if this is the last i-SAFE lesson to be implemented.
- Please submit photographs of students who create exceptional youth empowerment projects, for special recognition from i-SAFE. Photographs must be accompanied by corresponding personal release forms.
- We'd like to hear from you! Send an e-mail to teachers@isafe.org to share any unique ideas and/or experiences you had during implementation of this lesson.




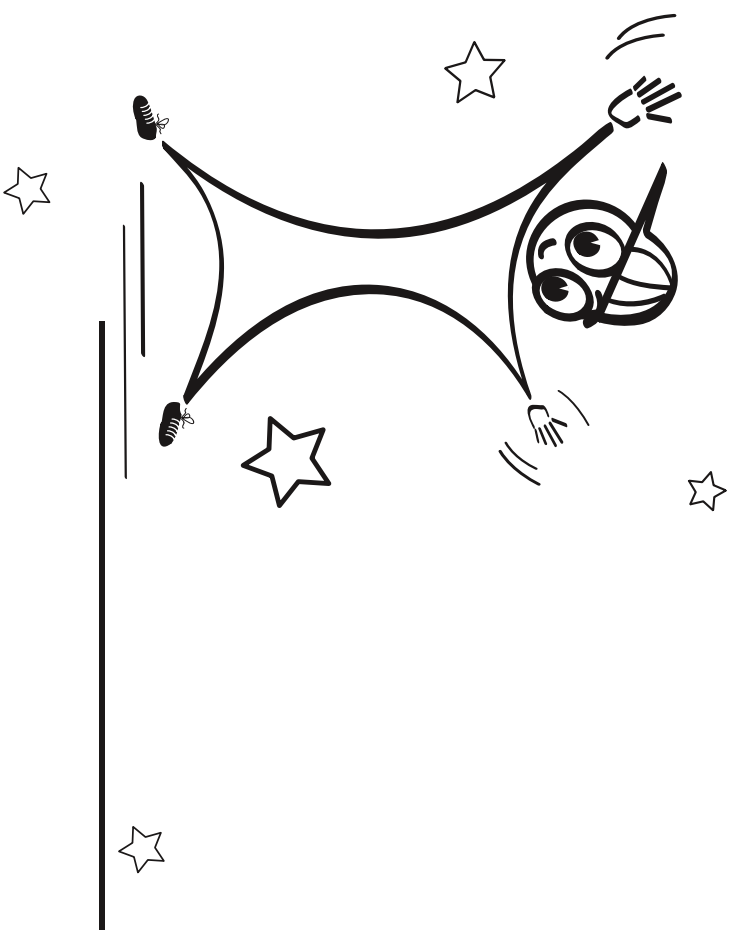
Name: _____


i-Buddy's Community

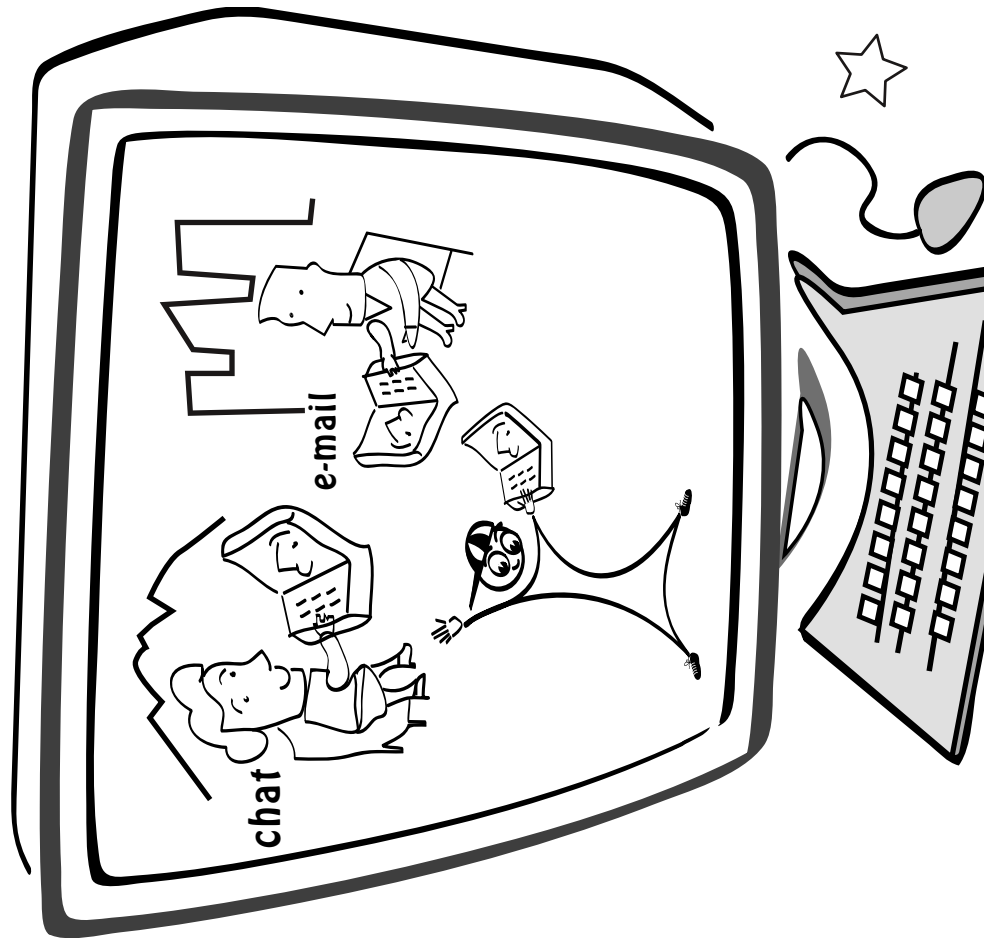




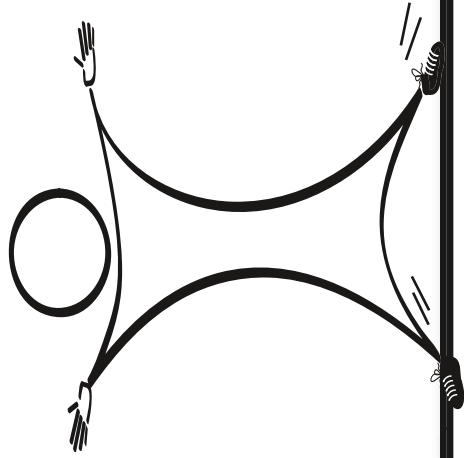
Our 
Community



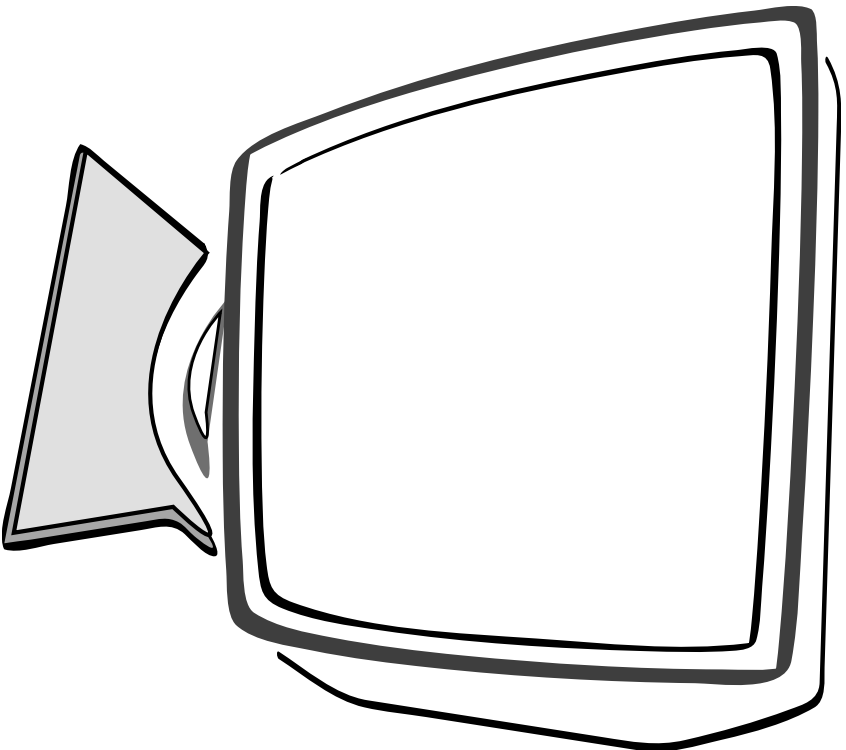
I am a
good citizen! 



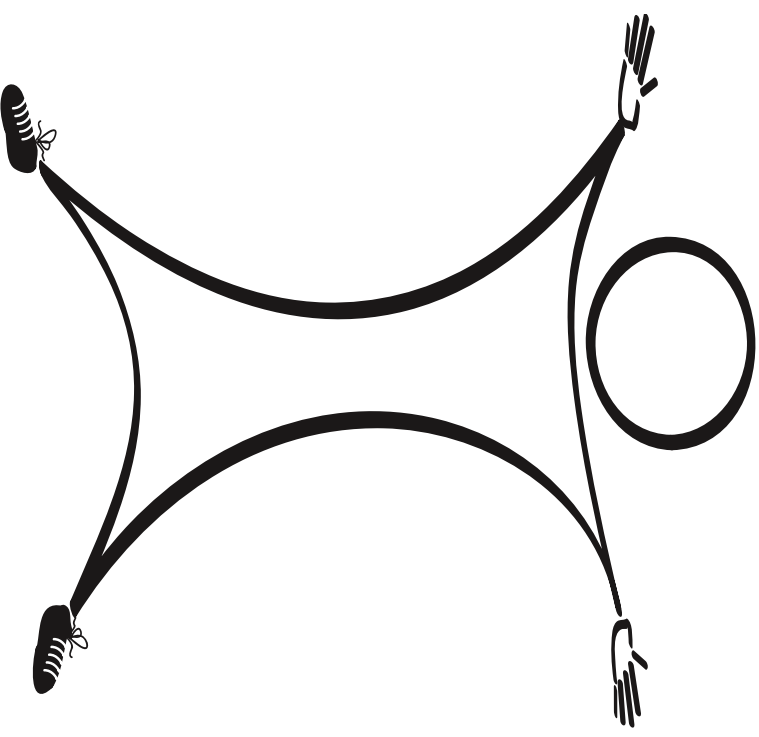
The Cyber Community



Call an adult
for help



**Traveling in
Cyberspace**



**It's not fun
to get lost**

LESSON—E-mail Safety Basics

Suggested grade levels k-2

This lesson introduces the concept that keeping young children safe requires having the help of a responsible adult when opening or sending e-mail.

Goal and Objectives

Students will:

- explore e-mail as a means for communication
- be introduced to the concept that computers can be damaged by e-mails containing computer viruses
- use the vocabulary terms: communication, e-mail, virus, and computer virus
- demonstrate an understanding of how to use e-mail safely
- share what has been learned with a family member

Materials

- a copy of the activity page for each student
- materials for drawing and coloring
- parent pages for each student

Procedures

Overview

Use the initial discussion to establish the students' general knowledge and experience level of e-mail use. Children's experience levels using e-mail varies. Even if children have not yet used e-mail, it is important for them to understand that a computer can be damaged through some of the activities it provides, and that people who use computers need to know prevention tips.

The lesson guide will give examples of information for the teacher to use as it fits the overall experience level of each unique class of students.

- The teacher will initiate and lead the discussion for each section.
- The first discussion examines what the students already know about the topic and serves as a guide for the rest of the lesson.
- After the initial discussion, students will complete their own knowledge charts to demonstrate what they have learned.

Discuss: Introduce the Topic

This discussion will cover a basic definition of electronic mail (e-mail) and will introduce students to the concept of responsibility in knowing how to keep a computer safe when opening or sending e-mail.

Briefly discuss the word communicate. What does "communicate" mean, and how do we communicate in the community we live in? (talk face to face, use phone, send letters, use the intercom)

Discuss: What Do We Know?

1. Ask the students to tell you what they already know about e-mail.

Lead the discussion to include the following:

- Electronic mail (e-mail) is a letter that is sent over the Internet.
- You can read an e-mail letter on your computer instead of getting it from the real mailbox.
- Sending e-mail messages is a great way to write to someone you and your parents know.

Summarize their findings, and ask them to repeat back to you.

2. Ask if anyone has heard of a computer virus. If they haven't, go to the next section. If students do know about computer viruses, have them share what they know. List items that you know are correct. Your list might look like this:

- A computer virus can be found in e-mail.
- A computer virus makes the computer work improperly.
- John's computer had a virus.

Discuss: What Do We Want to Know?

Use the topic and previous section as your guide to lead the discussion. Prompt the students to think about what would be important to know about using e-mail and computer viruses. Summarize their findings, and ask them to repeat back to you. Depending on the experience level, your summary might include the following:

- How do I send an e-mail?
- How can we see an e-mail virus?
- Is a computer virus a bad thing?
- What should we do about computer viruses in e-mail?

Discussion and Activity

Hand out the activity page to each student. Read the title "What I Know about Using E-mail Safely."

Explain that you will go over the page during the discussion, and they will have time to complete it at the end of the lesson.

Box 1

Read: When I have a virus, I am sick. **Ask:**

Does anyone know what a virus is? Provide time for student responses, and provide appropriate feedback. (A virus is a germ that can make you sick.)

Ask: How can people catch a virus, and what happens when they do?

Provide time for student responses, and provide appropriate feedback. Include:

- You can catch a virus from someone else's (an infected person's) germs when they cough or sneeze on you.
- When a person catches or becomes infected with a virus, he or she becomes sick.
- When you have a virus, you can't do the things you normally do because your body doesn't feel well enough to work properly.

Box 2

Read: When a computer has a virus, it won't work!

What did we say an e-mail is (a letter sent on the computer)?

Introduce or review: One way a computer can get a virus is through an e-mail. Cover the following:

- Sometimes people send a computer virus in an e-mail. The person might not even know the virus is there because it can be hidden in the message.
- What do you think about somebody who would send an e-mail on purpose that had a virus in it to hurt your computer? Provide time for student responses, and provide appropriate feedback.

Ask: Do you know how to keep viruses away from your computer? Provide time for student responses, and provide appropriate feedback.

Box 3

Instruct students to go to the last box and read: Be a hero! Ask an adult to help with e-mail.

Reinforce: The best way to keep your computer from catching a virus is to never try to open an e-mail message without help from a trusted adult (parent, teacher, or person designated by them).

That's the best way you can keep a computer virus from making your computer sick. You will be a hero for your whole family if you keep a virus from attacking your computer!

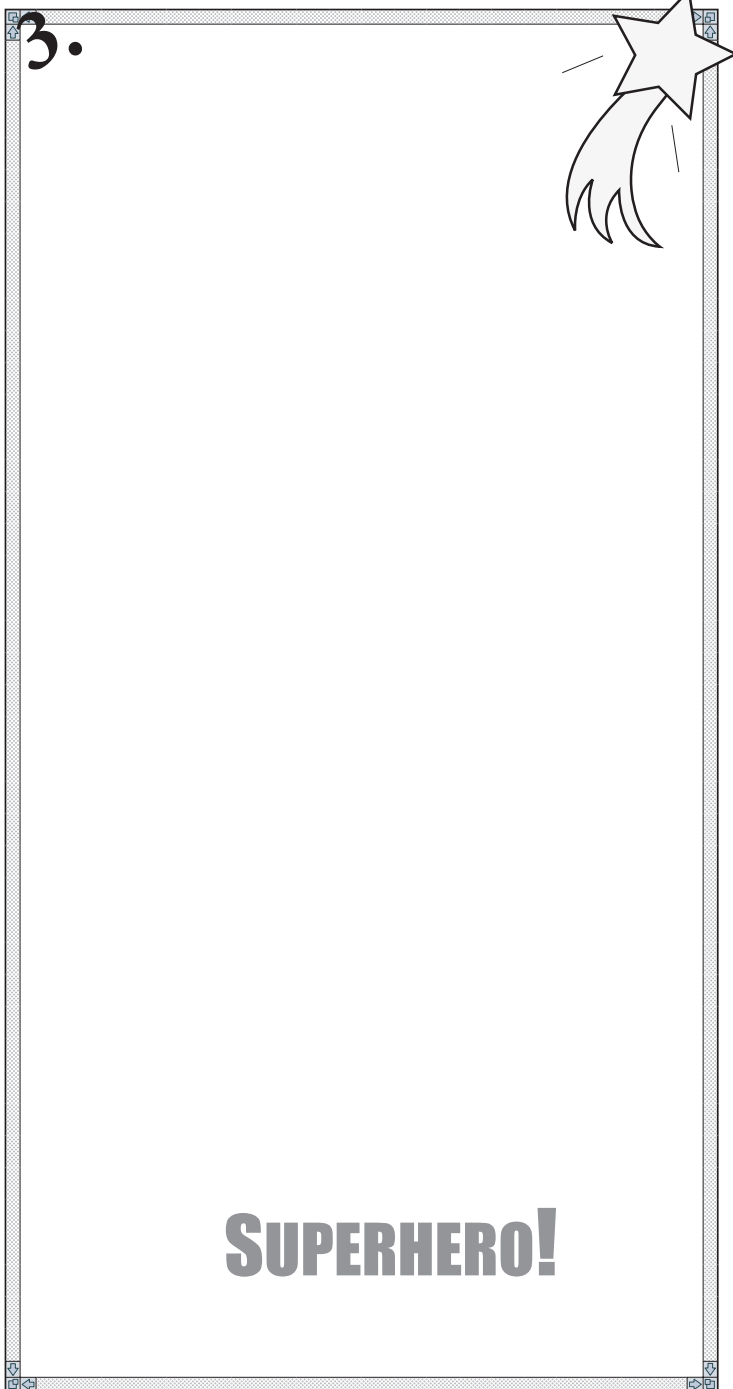
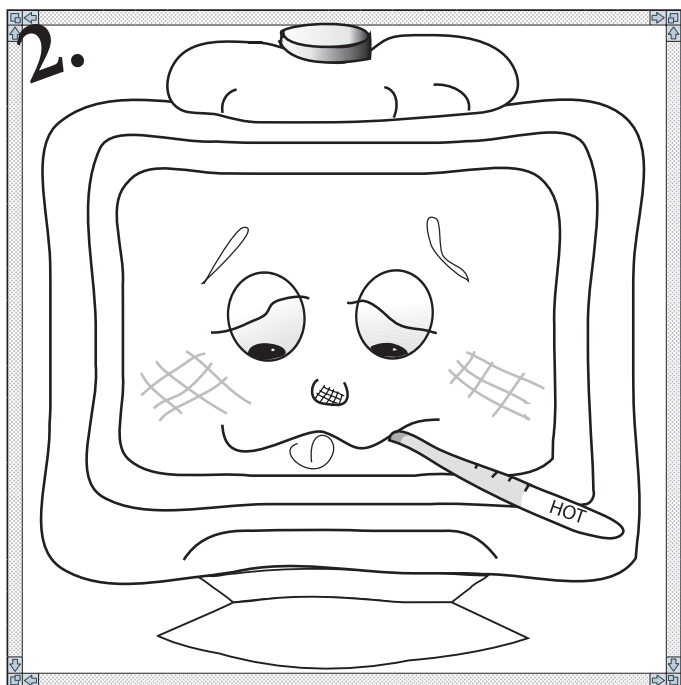
Activity page completion

- Box 1 – Draw a picture of how it feels to be sick.
- Box 2 – Color in the picture of the computer that does not work.
- Box 3 – Draw a picture of yourself being a hero.
- Explain the home link at the bottom of the activity page.

ACTIVITY—E-mail Safety Basics

Suggested grade levels k-2

Name _____ Date _____





GOING ON SAFARI



Learn About It

Traveling in the online community can be a lot like going on safari. You can explore places you've never been before, but you need to be careful too. You need to be aware of your surroundings at all times to avoid danger. i-Buddy and his cousin Jungle Buddy will guide you through this activity book to help you learn what to look out for and what to do if you see danger while "on safari" in Cyberspace.

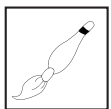


Read It

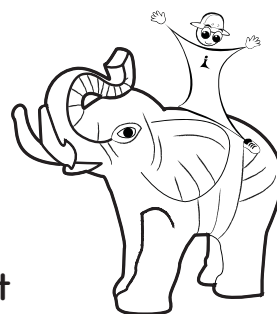
We usually think of our community as the area where we live, which contains places where we know real people. We find places in the community by their addresses, which usually contain a street number and street name. The Internet, also called Cyberspace, is also a community which contains places to visit, just like in the real community. A place in Cyberspace is called a Web site, and it has an address too, called a URL. Every time you are on a Web site, you can see its URL at the top of the screen.

Address

There are communities and places to visit all over the world, but traveling to foreign lands can take some time. The great thing about Cyberspace is that you can travel anywhere with a few clicks of a mouse.



Apply It!



Let's Go on Safari!

Let's say you are going on safari in the jungle. Write short answers to the following questions.

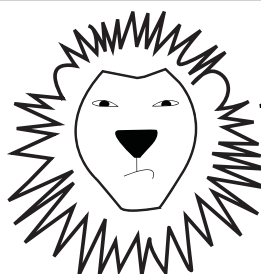
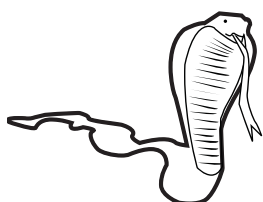
How will you travel in the jungle?

Will it be safer to go alone or with others?

What kinds of dangers do you think you need to watch out for in the jungle?

You have decided to hire a guide to help keep you from danger on the safari. What kinds of things do you want your guide to know?

How will you communicate with others back home to tell them about your travels?





Now think about an online safari.

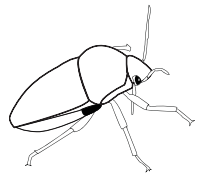
Think about how this kind of journey is like a real safari.

How will you travel in Cyberspace?

Will it be safer to go alone or with others?

What kinds of dangers do you think you need to watch out for in Cyberspace?

How will you communicate with others to tell them about your travels?



Words to know—You'll need to know the meanings of these words as we go along. Write any other new words you learn here too.

Cyberspace – the Internet

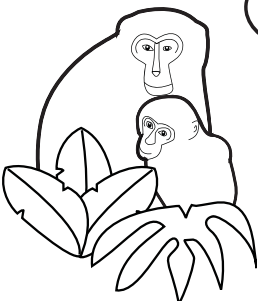
Safari – a journey or expedition

Aware – know about; be informed

Surroundings – that which is all around you

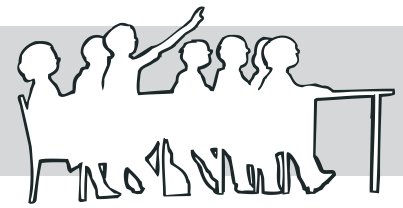
Appropriate – suitable; good for you

Inappropriate – not suitable; not good for you; unsafe



BE RESPONSIBLE with INTELLECTUAL PROPERTY

i-SAFE Intellectual Property Unit - Suggested Grade Level 4



UNIT Overview

This Intellectual property unit can be divided at sections indicated into shorter lessons. Some lessons are grade specific and others are available in each of the grades 3 – 4. Complete all lessons to ensure all necessary information on Intellectual property is covered.

Unit Content

- Cartoon featuring Donny the Downloader
- Intellectual Property Overview
- Intellectual Property Vocabulary Review
- Introduction to Piracy
- Cite Your Source Responsibly
- Build a Bulletin Board activity
- “Beat Street” take home activity page (can be used immediately after the i-SAFE Assembly Experience or as an activity for students who have not attended the assembly)
- i-Buddy Flash activity to reinforce Intellectual property concepts and vocabulary
- Sheet music for Beat Street theme song

Unit Goals

Note: Due to the abstract nature of the concepts in this unit, at this grade level, complete mastery of learning objectives is not expected. However, the introduction and development of the concepts will facilitate scaffolding of knowledge and understanding to enable mastery when appropriate.

This unit makes use of the characters: i-Buddy and Donny the Downloader, to enable critical thinking activities and to promote conceptual understanding of unit objectives. In this way students will:

- Be familiar with vocabulary terms related to the lessons
 - o Intellectual property
 - o copyright
 - o create
 - o creator
 - o copy and paste
 - o pirate
 - o piracy
 - o download
 - o legal
 - o illegal
 - o steal
- Understand that property on the Internet can be owned just like physical property
- Relate the term “Intellectual property” to something that is created in a person’s mind
- Associate different types of media as intellectual property: writings, music, videos, games, etc.
- Understand that there are rules/limits about making music CD copies for someone other than yourself
- Understand that it is stealing from real people if one copies CD and gives or sells them to others
- Understand that music on the internet is not always free for the taking
- Understand that there are rules/limits about downloading music from the Internet
- Understand that it is against the law to download music from the Internet without permission

- Understand that it is stealing from real people if one downloads music from the Internet without permission
- Know how to age-appropriately cite and Internet source for school work.



This icon will appear in student references and activities to indicate an opportunity to learn with Donny about the right ways to use intellectual property.

Empowerment Challenge

If any of these lessons are the first i-SAFE lesson, begin the Challenge.

Pass out the Empowerment Challenge page.

Instruct students to complete the Challenge for this lesson. Parents or teachers sign off on the challenge page. Students return the signed page to the teacher. Each lesson will include an empowerment challenge. When all lesson challenges have been completed, provide students with the DRiVE Learner's Permit.

Challenge Options

Note: The Challenge for Intellectual property lessons in grades 3 and 4 has been revised from earlier versions of the i-SAFE curriculum. Please sign off if students complete an appropriate activity from any lesson in this unit, even if it is not listed on the Challenge page. If this is the last challenge completed, provide students with the DRiVE Learner's Permit.

Option 1:

Students share their Intellectual property tips with another class or their families.

Option 2:

Students participate in building a bulletin board about Intellectual property.

Materials / Preparation

- Online access to the i-SAFE assessments, if any lesson in the unit is either the first or last lesson to be completed in the i-SAFE program
- A copy of activity pages for each student or student group as listed at the beginning of each lesson
- Computer access for flash activities (optional)

Assessments

Pre-assessment

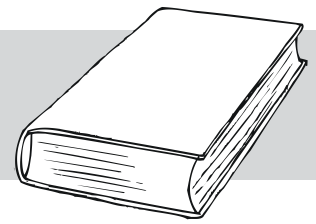
- When beginning the i-SAFE program with any lesson in this unit, administer the pre-assessment online at www.isafe.org by clicking on the link, "Assessments," prior to the lesson. Students will need to know their i-SAFE school ID# to obtain access.
- To verify school ID#, login at www.isafe.org go to your "My Info" page and select "Find your school ID."

Post-assessment

- When ending the i-SAFE program with any lesson in this unit, administer the post-assessment online at www.isafe.org by clicking on the link, "Assessments," following the lesson. Students will need to know the i-SAFE school ID# to obtain access.
- To verify school ID#, login at www.isafe.org go to your "My Info" page and select "Find your school ID."

LESSON PLAN— Intellectual Property

An Overview of Intellectual Property Concepts



Lesson Guide

Suggested grade level 4

This lesson introduces the basic meaning of Intellectual property and related concepts/vocabulary.

Learning Objectives

Students will:

- Develop an understanding that property on the Internet can be owned just like physical property
- Relate the term “Intellectual property” to something that is created in a person’s mind
- Associate different types of media as Intellectual property: writings, music, videos, games, etc.
- Develop an understanding that there are rules/limits about making music CD copies
- Develop an understanding that it is stealing from real people if someone copies CD’s and gives or sells them to others
- Develop an understanding that music on the Internet is not always free for the taking
- Develop an understanding that there are rules/limits about downloading music from the Internet
- Develop an understanding that it is against the law to download music from the Internet without permission from the copyright owner
- Develop an understanding that it is stealing from real people if someone downloads music from the Internet without permission from the copyright owner

Materials

- a copy of the activity page for each student
- materials for drawing and coloring

Procedures

This lesson makes use of the character: Donny the Downloader, to promote critical thinking activities and to promote conceptual understanding of lesson objectives.

Read the following script to introduce (or review) concepts.

“Today, a character named Donny the Downloader is going to help you learn about something called **intellectual property**. We are going to learn when it is okay to use information and things you find online and when it’s wrong and even against the law to do so.”

“Today you are going to learn about **Intellectual property**. We are going to learn when it is okay to use information and things you find online and when it’s wrong and even against the law to do so.”

“First of all - Let’s see how much you already know!”

Question: “What is Property?”

Provide time for students to respond. (Items with value that we own—examples include shoes, books, a car). Provide positive feedback as the students properly identify Intellectual property items and help develop a definition.

Then add: “Property is something that has value. It is owned and sometimes you can buy or sell it. But what about things you can’t touch; like the name *Disney* or the words to a song?”

Question: “Can Property that you can’t touch be worth money? Can you give examples?” *Provide time for student responses.*

Intellectual Property on the Internet

“There is no difference between Intellectual property found on the Internet and writing or pictures you would find in a book or magazine. Someone put their own writing and work on the Internet to let other people read it and see it. It was not put there for other people to copy and say it belongs to them. It belongs to the person who created it.”

Provide time for students to think of other things on the Internet that are intellectual property.



Example: “You have probably purchased a CD, and maybe your parents own a picture. You can touch those things. But what about if a song from the CD and the same picture is on the computer (on the Internet)? Are they still property then?”

Provide time for student input about whether items online are property.

Question: What does it mean to “steal” something? (*Answers should include: take something that belongs to someone else or without paying for it.*)

Use the following open-ended questions:

- Review the topic of Intellectual property by asking: What is property (something of value that is owned, which can be bought or sold)? Have students give examples of physical property they own.
- Ask students if they need to be able to touch something for it to have value? (*Introduce examples—Disney, a song lyric, etc. Ask students if they are worth money, etc. Explain that these are also property.*)
- Introduce the term Intellectual property. Intellectual property is any intangible asset formulated from human knowledge and ideas. Intangible means it can’t be touched.
- Identify various types of Intellectual property. Ask students to contribute by volunteering their ideas. Tell students to brainstorm intellectual property that they have thought up.
- Review with students that when Intellectual property is put into tangible form it is protected by copyright.
- Review with students. A creator can create a work in their head. That could be an idea for a picture, song lyrics, a story, etc. This is Intellectual property. Once the creator puts the work into some type of tangible form it is a type of property that is protected by copyright.
- Ask students what it is called when someone downloads music illegally online – piracy.
- Reinforce that there are laws that protect property online and when they take something online by downloading, copying, cutting and pasting, etc without purchasing or asking permission they are stealing.

Reinforce:

“There are laws against copying things that other people have created or made. We call that “against the law”. It is stealing from real people if you copy things that don’t belong to you.”

Activity



Explain that in this activity, this icon will mean that it is a chance to learn with Donny the Downloader about the right ways to use Intellectual property.

- Provide each student with a reference page
- Allow some time for student to read it and color if desired.
- Go over the information together.
- Have students share their rules with the rest of the class.

ACTIVITY—Making the Right Choices Online



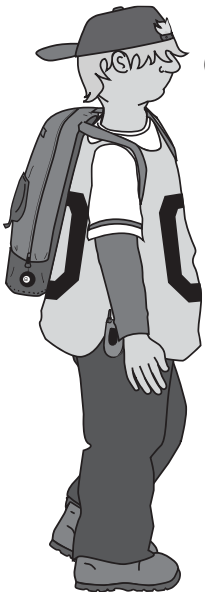
What's the Big Deal?

Intellectual property is something real – it belongs to the person who created it.

- If you take it for yourself without paying or without getting permission from the owner, you are stealing from a real person.
- Stealing from the Internet is just like stealing from a store.

Beat Street RULZ

- Don't download illegally (that's without paying or getting permission).
 - You might hurt somebody!
- DO find legal places to download music.
 - Online music is COOL!
- It's UNCOOL to break the law by copying CDs, but you CAN make a personal copy for yourself.



Create your own rule here:

LESSON—Text Messaging Safety

Suggested grade levels 5-6

Lesson Guide

Students will become more familiar with online communication and its personal and security consequences related to text or instant messaging (IM). This includes developing an understanding of the need for basic safety rules and netiquette usage when instant messaging.

Learning Objectives

Students will:

- understand text and instant messaging and their associated vocabulary
- understand the need for basic safety rules and netiquette usage when text or instant messaging

Materials

- resource page for each student
- activity page for each student group
- parent tip sheet for each student

Procedures

Discussion

- Ensure that all students have printouts of the newsletter reference page and the informational page on netiquette.
- Engage students in a brief discussion in which they identify how and why they use instant messaging and/or text messaging. Use the following to guide the discussion:
 - > How many students use IM and/or text messaging?
 - > Why is IM so popular?
 - > List some personal dangers in conversing via IM (cyber bullying, misconstruing comments, grooming by predators, etc.).
 - > List some computer security dangers in conversing via IM and/or text (attachments containing computer viruses, Trojan horses, spyware, etc.).
- **Informal Poll:** Take an informal poll of students regarding how much time they spend instant messaging each day, week, or month.
- Compare and contrast communication in the physical and online communities (specifically via messaging). Cover the following:
 - > the different rules for online communication
 - > the need to be more careful in online communication (can't see each other, may not have met physically)
- Read the reference sheet on instant/text messaging as a class.



Discussion 2

- Discuss the term netiquette.
 - > Ask students to define netiquette.
 - > **Netiquette:** informal rules of Internet etiquette or how to behave in a polite way online
 - > Ask why netiquette is necessary for safe and secure online communication.
 - > Ask how netiquette can help preserve computer security.
- **Ask:** What is the effect of netiquette on cyber bullying and other online dangers? Discuss.
- Stress that just as there are guidelines for how to act and behave in the physical community, the online community has similar unofficial rules in place.
- **Ask students:** What happens when someone breaks guidelines or social rules in the physical community (can be ostracized, punished, fewer friends, etc.)?
- **Ask students:** What could happen if you break the guidelines or social rules in the online community?

Group Activity – Netiquette Rules

1. Divide students into small groups, and hand out the reference sheets.
2. In their small groups, students should brainstorm some basic rules of netiquette for instant messaging.

Presentations and Discussions

1. Students should present their netiquette rules to the class.
2. Discuss the rules and what students have learned about safer text messaging as a class.

Children who participate in activities and share what they have learned about Internet safety are more likely to practice safe habits online.

Additional materials and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. E-mail international@isafe.org for more information.

REFERENCE—Text Messaging Information Sheet

Suggested grade levels 5-6

Instant Messages (IM): notes back and forth with someone who is online in real time

Instant or text messaging are easy ways to communicate! However, there are dangers that should be considered when texting.

Buddy List:

Just who are the people on your buddy list? Some people consider it a status symbol to have the most “buddies.” Do you really know them, or did you just meet them online?

Tip: Be careful about who you add to your list!

The Instant-Messaging Profile:

When signing up for the typical instant-messaging software service, people are asked to complete a profile. This profile can ask for information like name, hobbies, and address. This profile is then available to anyone who wishes to IM you. Even worse—anyone can do a search to locate profiles of people based on characteristics. They can click on your name and read your profile. For predators and others, this information can be used inappropriately.

Tip: Choose not to fill out your profile or make sure to leave out any personal or identifying information.

Cyber Harassment:

Unfortunately, the very features that make instant and text messaging so user friendly and fun also make it a great tool for cyber bullies and harassers. Via cell phone, harassment can occur 24/7. Another issue to consider is that instant-message harassers are alerted via their buddy list when their victims are online.

Tip: Victims of online bullies need to be aware of how to block harassers, keep records of harassment, and most importantly, get help—even if that means going to multiple sources before help is received.

Malicious Code:

One great aspect of instant messaging is that it allows for not just the transfer of text messages but also the transfer of files. Unfortunately, that means instant messengers can transfer worms and other malware. Hackers can use instant messaging to gain access to computers, bypassing most firewalls. Another concern is that many IM networks bypass safety and security precautions like firewalls, virus-protection software, and filters.

Use text messaging, but use it safely!

ACTIVITY—Netiquette Rules

Name _____ Date _____

Netiquette: informal rules of Internet etiquette or how to behave in a polite way online

In small groups, brainstorm a list of five netiquette rules that apply to instant messaging (IM). Present these rules to your class when finished.

1.

2.

3.

4.

5.

i-SAFE ONLINE PERSONAL SAFETY UNIT - OVERVIEW

Suggested Grade Level – 6

curricular guide with options for classes with or without computers

Overview

The “Personal Safety” lesson unit consists of four separate lessons combined into one unit. The unit can be completed as one longer lesson or divided at the lesson component sections indicated into shorter lessons. Complete all four lessons to ensure all necessary information on online personal safety is covered.

Note: Component 3 of this unit briefly touches on online strangers, predators, and the grooming process. If appropriate to your students, the lesson “Predator Identification,” available in the “Predator Identification” module, provides more in-depth coverage of this topic.

Unit Goals

Students will

- recognize ways personal information provided on the Internet can be used to harm the user
- make responsible choices in what they reveal online
- revise screen/user names and/or passwords to apply safety standards, if needed
- refuse to communicate with strangers who exhibit grooming tactics
- refuse to meet face to face with Internet strangers without the permission from parents
- recognize and report suspicious behavior by an online stranger to a trusted adult
- communicate in Cyberspace safely

Enrichment Goal

i-SAFE enrichment activities are to be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at www.isafe.org.

Completion of this unit will prepare and guide learners to create and distribute brochures to create awareness about online personal safety.

Materials/Preparation

- online access to the i-SAFE assessments, if appropriate for this lesson
- a copy of “Be Smart – Be Safe” activity pages for each student
- a copy of the teacher resource article
- a bingo card copy for each student
- a copy of the information game page, cut up as directed for group activity
- computer access to desktop publishing for creating a brochure or provided MS Word brochure template (optional for use in classrooms with computers)
- student registration in i-MENTOR program at www.isafe.org
- optional: PowerPoint presentation available for use as a student guide

UNIT EXCERPT: Lesson 2 – Protecting Personal Information

Learning Objectives

Students will:

- comprehend that anyone met exclusively online is a stranger
- understand how indirect information can be used to identify someone
- recognize how to respond appropriately to Internet strangers
- understand risks of providing too much personal information in online profiles and forms

Read and Discuss

- Read the resource article located at the end of this lesson plan to the class.
- Have the group brainstorm how this could have been prevented.
- Have students answer the following questions:
 - Why do students feel safe on the Internet?
possible reasons: in own home, behind screen, anonymous, etc.
 - What are some dangers on the Internet?
possible answers: predators, thieves, bullying, bad sites, hate sites, etc.
 - What are some good things on the Internet?
possible answers: research, information, ability to find things, maps, directions, etc.
- Provide each student with a copy of the resource page, and select students to read the information to the class.
- Discuss and/or answer any questions about direct and indirect information.

Bingo Game

The following activity reviews and reinforces the concepts learned in this lesson and Lesson 1 of the personal safety unit. As you play the game, make sure to reinforce key lesson points, such as never revealing personal information online.

- “We’ve covered an enormous amount of information. Now you’re going to have an opportunity to show how much you have learned. This activity is called ‘REVIEW BINGO’.”
- Distribute the “REVIEW BINGO” sheets, and ask students to read the directions with you. Then have students fill in answers on their bingo cards working alone, in pairs, or in small groups.
- When students finish filling out their bingo cards, announce: “Now I’ll draw slips of paper that will have questions. These questions are answered by the words on your bingo square. After the question has been called, place a large check mark (or scrap of paper) in that bingo square. When you have checks in five boxes in a row or diagonal, call out “Bingo!” At that time, I will review with the class the correct answers to all of the questions asked and make sure your card was correct. Any questions?”
- As you play the bingo game, clarify and/or discuss terms or information that students find difficult.
- After winners have been identified, hold a brief discussion of the answers for squares not called in the activity.

-
- This game can be played multiple times or as time permits. If the game will be replayed, use colored paper or some other way to mark squares.

Wrap-Up Discussion

- Review with students the necessity of choosing anonymous screen names and passwords.
 - Reinforce that personal/identifying information should never be revealed online.
 - Remind students that anyone met online is a stranger.
-

Resource Article

The following article is based on a compilation of several real stories about Internet safety issues.

Most teenagers and young adults these days have been online. Certainly there are plenty of good reasons to use the Internet—hanging out with friends, doing research, and playing games. Unfortunately, there is increasing danger involved in getting online.

Take Brittany for example. Brittany was a young teenager. She liked to hangout, play softball, and chat on the Internet, especially with Jason, the friend she met while online. Even though they had never met in person, she just knew Jason was her soul mate. He liked everything she liked, and they could always talk about softball. He knew her school and her team number. She had described the new uniforms to him.

Jason had reminded Brittany about being careful—to be careful about giving out personal information online. He cared about her and wanted her to be safe. As a matter of fact, he had reminded her so often that she tended to tune him out. To her, it wasn't like she chatted with anyone she didn't know! Besides, she never gave out her home address or phone number.

Brittany felt safe online. However, she wasn't fully aware of all of the dangers out there. Even without sharing her address, Brittany had supplied Jason with enough information in their conversations for him to be able to find her offline. And more importantly, Jason had built a trusting relationship with her, even though they had never met.

Fortunately, Brittany's friend was, in reality, a 35-year-old law-enforcement officer who was involved with the prevention of Internet crimes. Establishing an Internet relationship with Brittany was used to show how easy it is for people on the Internet to get information that can potentially put others—especially young people—in danger. Demonstrations like this one have been used across the country to show that only until you know what the dangers are, and know how to protect yourself, can you be assured that you will have a great time online, and still be safe.

Who knows WHAT about You?

Know about indirect information solicitation

Sometimes people can find out all about you “indirectly” – by piecing bits of seemingly unrelated information together. For example, indirect information about your school, activities, etc., could lead someone to figure out where you live. Be aware of **what you say** at all times, and **where you say it** online –

Watch out for communication dangers...

... on the Web

- **POP-UPS** – You are a WINNER! Surfing the Web often provides lots of pop-ups offering free merchandise, contests, and survey forms to fill out. Information you provide can be used to create email spam and will make MORE pop-ups!
- **Websites you visit** – Some websites ask you for private information before you can access their stuff. Make sure you ask your parents before giving anyone private information on online forms.
- **Your own website** – Many young people now have their own Websites or social networking pages. Be cautious about what information you display.

...in E-mail

- Spam – many companies advertise via e-mail and ask for more information about you. Do not respond to these emails – DELETE them!
- Be careful when you reply to an e-mail. You are including your e-mail address and you don't know where it will go from there.
- Remember the sender of an e-mail may not be someone you know – don't send personal information, photographs, etc.

...when Chatting, IMing, or Gaming

Instant communication can result in revealing information you wouldn't normally reveal. This can leave you open to harm.

- Keep online interaction online. Don't agree to meet or phone people met online.
- Don't give out personal information. Be careful about indirectly saying too much about yourself. Eventually you will have said enough.
- Private chats aren't always private – when you meet offline friends online in a private chat room, be careful. Others can often enter and lurk (watch what you are saying about yourself).

Directions: Using the word sheet, fill in the squares of the bingo card below. Mix up the words so that your card isn't the same as someone else's. The teacher will read out questions. The answers to these questions are those words you used to fill in the bingo squares. Find the correct answer and mark it off. You have Bingo if you get five in a row. Raise your hand or call out Bingo when you do!

Internet Safety Bingo				
		FREE		

Bingo Vocabulary

Directions: Use the following twenty-four words to fill in the squares on your bingo chart. Remember to mix up the order of the words – you don't want your chart to look like anybody else's. Then to play the game, listen carefully as the teacher reads out questions. Try to locate the correct answer to the question and mark it off on your bingo chart. When you get five in a row horizontally, vertically, or diagonally – call out Bingo!

Vocabulary:

1. LMSmith14
2. Singin4fun
3. Chat
4. Pop-ups
5. Address
6. Password
7. Spam
8. Delete
9. Trusted adult
10. Indirect
11. Stranger
12. Screen name
13. Online form
14. IM
15. 19#He%d2
16. Personal Information
17. Online
18. Picture
19. Your own Webpage
20. Change it
21. False
22. True
23. Unsafe
24. Anonymous

Teacher Resource Page: BINGO Terms and Definitions

1. this is an example of a screen name that is considered inappropriate.
LMSmith14
2. This is an example of an appropriate screen name.
Singin4fun
3. This is a way to communicate online.
Chat
4. Providing information on these will give you spam email and more of these.
Pop-ups
5. This is one piece of information, which is considered private or personal.
Address
6. You should never tell this information to anyone or even write it down.
Password
7. This refers to unwanted garbage e-mail
Spam
8. You should do this when you receive unwanted email.
Delete
9. When you feel you or a friend are in danger from someone from the Internet you should report it to a
Trusted adult.
10. This refers to the kind of information that is gained through knowing things like a school mascot, concerts, etc.
Indirect
11. A person you have only met on the Internet is a
Stranger.
12. An online nickname is also known as a
Screen name.
13. Ask a parent before you fill out one of these.
Online form

Page 2 – BINGO Terms and Definitions

14. The well-known abbreviation for Instant Messaging is **IM.**
15. This is an example of a safe password.
19#He%d2
16. First or last names, phone number, and birth date are all examples of **Personal Information.**
17. Do not meet or phone people you meet **Online.**
18. It is dangerous to send this or post this online.
Picture
19. You should be careful about personal information you put here.
Your own Webpage
20. What should you do if you think someone knows your password?
Change it
21. True or false: It is a good idea to give your phone number to people you meet online.
False
22. True or false: It is a good idea to keep your parents or guardians informed of online interaction.
True
23. A screen name containing your zip code, your school name, and your last name is **Unsafe.**
24. If your screen name/user ID contains personal information, you are NOT **Anonymous.**

i-SAFE Cyber Security Unit

Suggested Grade Level – 7

SAFETY

Curricular guide with options for classes with or without computers

UNIT Overview

The Cyber Security lesson unit consists of four separate lessons combined into one unit. The unit can be completed as one longer lesson, or divided at the lesson component sections indicated into shorter lessons. Complete all four lessons to ensure all necessary information on online security is covered.

PowerPoint Review Lesson – This option provides the key unit concepts in a PowerPoint presentation format.

Unit Content

- Malware Issues
- Acceptable Use Policies
- Risks of Spyware
- National Student Watch
- Cyber Security Review PowerPoint Lesson—covers key concepts from this unit



Unit Goals

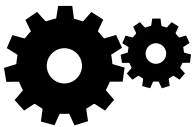
Students will:

- develop an understanding of malware issues and how they affect e-mail protocol
- understand the necessity of using caution when opening e-mail to protect computer security
- inform others about cyber security issues
- examine necessary components of an acceptable use policy (AUP)
- review the school's AUP
- develop AUP guidelines
- understand the term spyware and the types of programs it applies to
- understand the security risks associated with downloading items online
- understand how personal information may be compromised via spyware
- understand their schools action or disaster plan in response to homeland security threats and how to communicate threats



Enrichment Goal

i-SAFE enrichment activities are designed to be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at www.isafe.org.



Enrichment Activity

Completion of this unit will prepare and guide learners to create a skit or other presentation for their school on a selection of cyber security topics.

Materials / Preparation

- | | |
|--|---|
| <ul style="list-style-type: none">• online access to the i-SAFE assessments, if appropriate for this lesson• copies of the reference pages for each student• copies of the activity pages for each student• computer access for HTML activities (optional)• copies of the school's AUP for each student group• student registration in mentor program at www.isafe.org | <ul style="list-style-type: none">• copies of the school's AUP for each student group• student registration in mentor program at www.isafe.org• <i>optional</i>: PowerPoint access for review lesson |
|--|---|

Pre Assessment

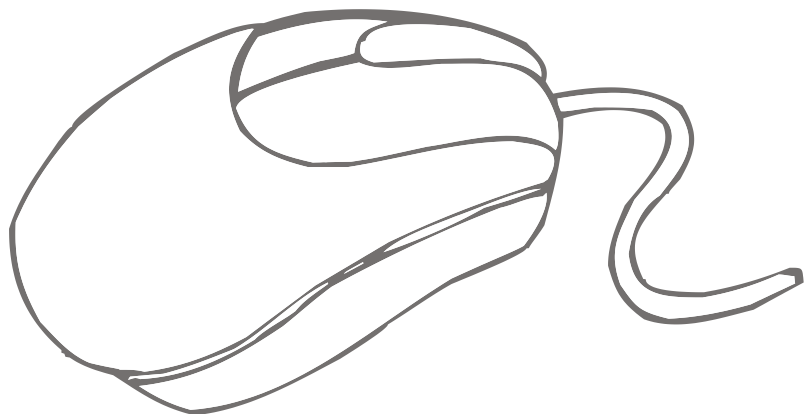
- If beginning the i-SAFE program with any lesson in this unit, administer the pre assessment online at www.isafe.org by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at www.isafe.org, go to your “My Info” page and select “Find your school ID”.

Post Assessment

- If ending the i-SAFE program with any lesson in this unit, administer the post assessment online at www.isafe.org by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at www.isafe.org, go to your “My Info” page and select “Find your school ID”.

Mentors

All students participating in the i-SAFE curriculum are considered i-MENTORs. If they haven't done so already, have students enroll online by clicking on “Create Account” at www.isafe.org to take full advantage of the support and incentives offered. This may be done at any time during the lessons, or students may complete this registration at home.



LESSON 1—Malware Issues

Suggested Grade Level – 7



Learning Objectives

Students will:

- develop an understanding of malware issues and how they affect e-mail protocol
- understand the necessity of using caution when opening e-mail to protect computer security
- inform others about cyber security issues

Discussion 1

- Review with the students that there is an online cyber community. Ask students what some of the benefits are of an online community.
- Ask students to think of some of the negative sides of an online community. Lead into informing students that they will be addressing a particular negative in the online community: Malware – programs, such as worms and viruses, that include “malicious code”.
- Ask students how many have ever had their computer crash because of a virus?
- Ask students if they know how viruses are spread?
- Ask students for their definition of viruses. Discuss their ideas. Provide students with the following definition of viruses: A virus is a computer programs that is designed to replicate by copying itself into the other programs stored in a computer. It may have a negative effect, such as causing a program to operate incorrectly or corrupting a computer’s memory.
- Discuss some of the viruses they may have heard of.
- Inform students that one common method of obtaining a virus is by downloading an attachment from e-mail.
- Ask students what their own experiences with e-mail have been. What common issues, annoyances, etc. have they run into?

Peer-to-Peer Activity

Choose one (1) of the following options: for classrooms with computers or for classrooms without computers, to accommodate different classroom environments.

With Computers

If working in a computer lab, allow students to access the HTML activity on their computers. Students can work individually, in pairs, or in small groups. Allow your situation to dictate guidelines. You are authorized by i-SAFE to reproduce the files in any way appropriate for providing individual computer access in your learning environment, such as CD, disk, hard drive copies, or network availability.

- This activity walks students through the concepts of viruses, worms, and Trojan horses. It explains how these are spread and how to prevent infecting a computer. When finished with the lesson, students enter a scenario game. They are asked to choose how they would react to various situations.
- The pages provide directions and information on viruses and will lead into the activity of writing a scenario/skit.
- Proceed to Scenario and Skit writing.

Without Computers

- Divide students into small groups and hand out the Reference page.
- In their small groups, students should read and discuss the information on malicious code and computer viruses.
- Proceed to Scenario and Skit writing.

Scenario and Skit Writing

Provide students with the skit writing handout.

Using what students have learned from their group work, they will write a scenario or skit that includes the presentation of a problem associated with the topic and an appropriate solution.

Skit Presentations and Discussions

- Students should present their short skits to the class.
- As a class, discuss the skits and what students have learned about malicious code and viruses.

Note – this activity may be used as a final enrichment activity.

Concluding Discussion

- Review with students what malicious code is and the necessity for precautions when online.
- Discuss why it is important to discuss cyber security issues with others and how to be proactive in dealing with it.



REFERENCE—Malicious Programs



Malware – Malware are programs, such as worms and viruses, that include malicious code—code written with the intent to harm, destroy, or annoy. “Code” is a term for the language(s) computer programs are written in—the “code” tells the computer what and how to do things. Malware can attach to e-mail and carry out their programming which can cause computers to work improperly.

A **Virus** is a computer program that spreads itself by infecting files. Viruses are dangerous and can shut your computer down. While there are many ways to get a virus, the most common is through downloading e-mail attachments.

- There are consequences for creating or spreading a virus. You can be prosecuted as a criminal.

Worms also include malicious code. Worms work through networks. They travel through shared files and programs and can bring down an entire system.

Trojan horses are another type of malicious code. These are programs that claim to do one thing but actually do another when downloaded. For example, you download a game but instead the program wipes out your hard drive.

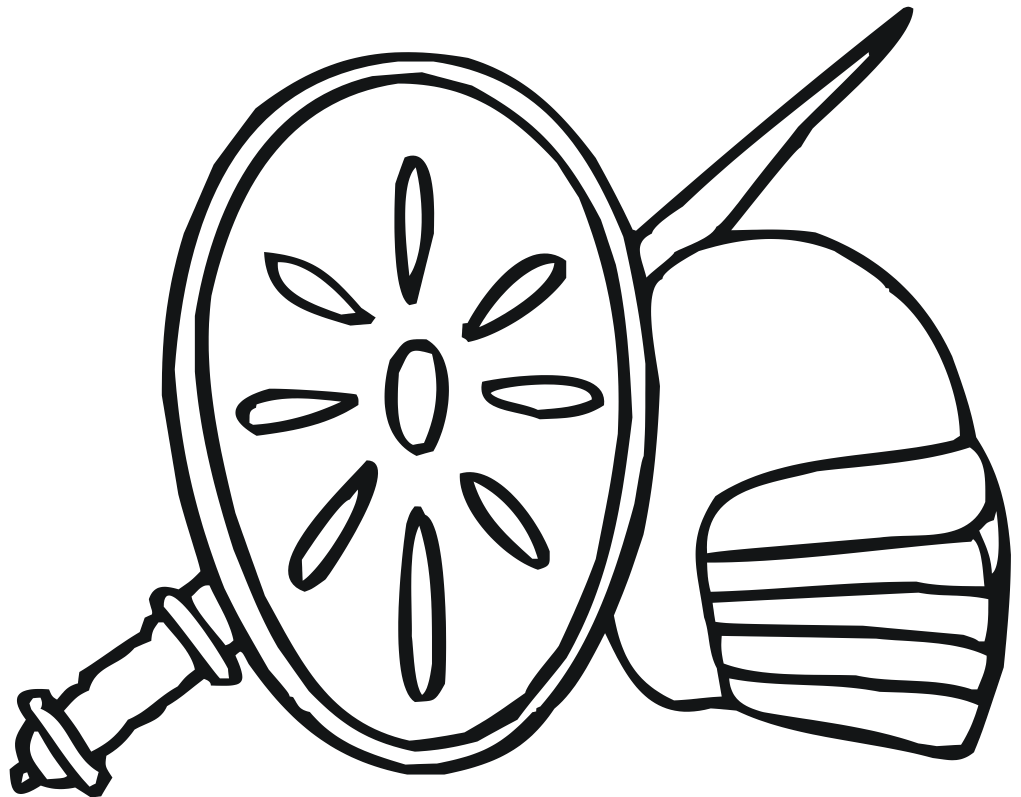
Spyware A program running in the background to monitor your computer activities. Frequently downloaded without you knowing it, they can monitor your web browsing and cause pop-ups.



Prevention Tips

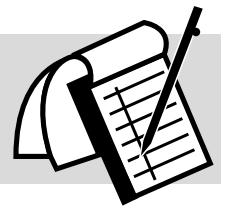
Here are some things you can do to keep your computer safe and keep it from being a threat to other computers:

1. Make sure a firewall is installed on your computer. If you aren't sure, ask your parents. A firewall prevents information from entering your computer without your permission.
2. Keep your computer updated (download updates for your operating system regularly)
3. Install anti-virus software on your computer, keep it updated, and most importantly—USE it.
4. Install anti-spyware software on your computer and run it periodically.
5. E-mail that has been forwarded "FW:" or has an attachment with the suffix of ".exe," ".scr," or ".vbs." should be considered a red flag for possible virus infection. If you do want to open an attachment, scan it through the virus software first. To do this, save all attachments before opening them.



LESSON 2—Acceptable Use Policies

Suggested Grade Level – 7



Learning Objectives

Students will:

- examine necessary components of an acceptable use policy (AUP)
- review the school's AUP
- develop AUP guidelines

Take a Poll

Have students conduct an informal poll of students at their school regarding the school's Acceptable Use Policy (AUP).

- Do students know what the AUP is?
- Did students sign an AUP?
- Did the student's parents sign the AUP?
- Do they know what is in the AUP that pertains to them?

Discussion 1

Note: for an additional teacher resource, access the Dig Deeper on Aups at http://www.isafe.org/channels/sub.php?ch=ed&sub_id=2#digdeeper

- Ensure that all students have printouts of the AUP activity sheet.
- Engage the learners in a brief discussion in which they define the term AUP (Acceptable Use Policy). Guide the discussion to cover the following:
 - > Why should schools have an AUP in place?
 - > Why do students, parents and teachers need to be educated on the AUP?
 - > What do you think should be covered in an AUP?
- Have the students refer to the reference sheet: Acceptable Use Policies. Read over the information provided on the sheet.
- Brainstorm!
 - > Allow students a few minutes to brainstorm on this topic before proceeding to read what i-SAFE feels should be included in an AUP.
- Review the information covered in the activity sheet as a class.

Create student groups of 3 or 4 to complete the following project.

Peer-to-Peer Activity

Direct the students to engage in the following activity. (This group activity can also be done as a class on overheads if preferred)

- Each group should receive a copy of the school/district Acceptable Use Policy for review.
- Each group should receive a copy of the Acceptable use Policy Rubric.
- Have each group work together to review the school's AUP using the rubric as a guide.
- Have each group come up with a list of three suggested revisions to the school's AUP based upon what they have learned during the course of the lesson.
- Proceed to Discussion 2.

Discussion 2

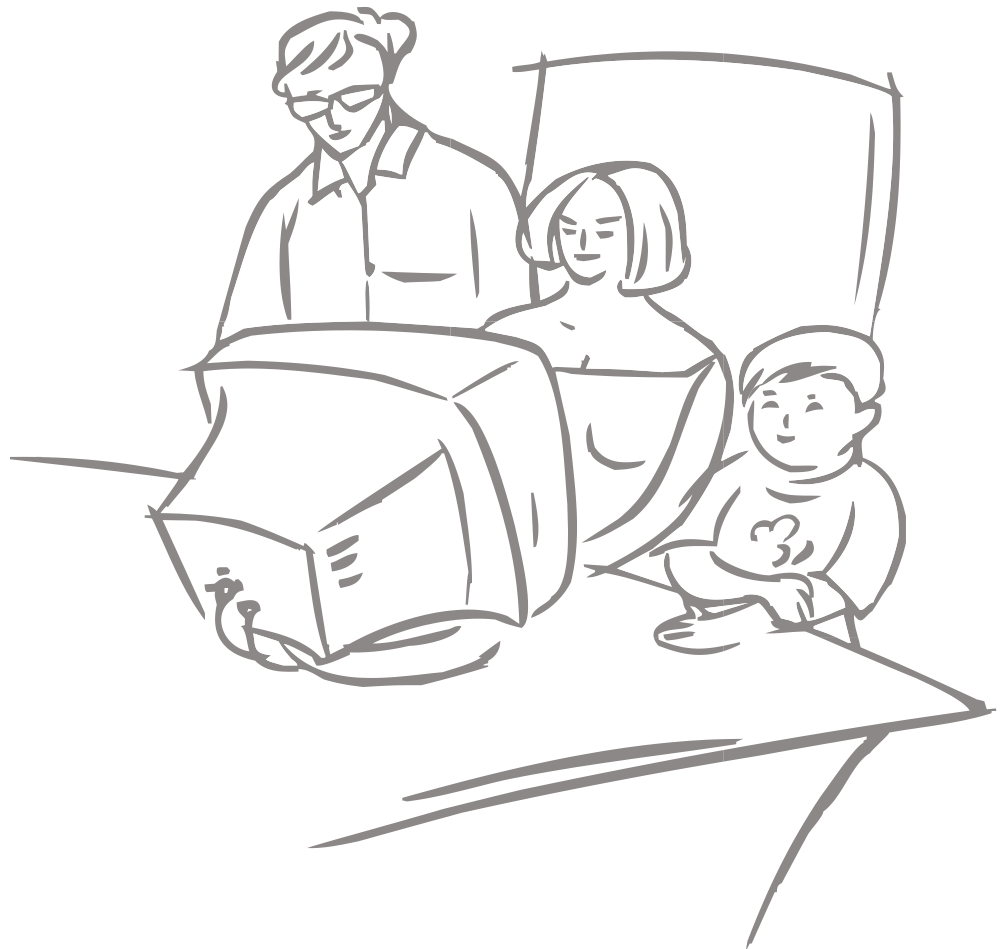
Provide time for the student groups to present their evaluations, and discuss. Once presentations are finished, discuss:

- Does your school's AUP cover all necessary information?
- What could be added to the school's AUP to make it better?
- Should any changes be made to the AUP?

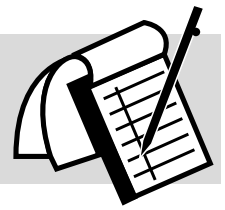
Concluding Discussion

As a class, discuss the following:

- Review what an Acceptable Use Policy is, the necessity for AUPs, and critical components of your school's AUP.
- Ask students why it is necessary to make the information of your school's AUP known to others such as faculty, students, parents, etc.
- Ask students how this information can be more publicized.



ACTIVITY—Acceptable Use Policy Rubric



	Yes	No	Comments
General:			
1. States acceptable uses for computers.			
2. States unacceptable uses for computers.			
3. States privileges of use.			
4. States consequences of abuse.			
5. Covers network etiquette.			
6. Contains a code of conduct for Internet usage.			
7. Contains a list of the responsibilities of educators, parents, and students for using the Internet.			
8. Includes a description of the instructional philosophies and strategies to be supported by Internet access in schools.			
9. Incorporates a statement on the educational uses and advantages of the Internet in your school or division.			
10. Has section for both student and parent signatures.			

BRAINSTORM:

What are three possible revisions that could be made to your school's AUP to make it better?

1.

2.

3.

ACTIVITY—Acceptable Use Policy (AUP)



AUP:

An AUP is what is known as an Acceptable Use Policy. It lets you know as the student what is acceptable when using the Internet at your school. It should teach you acceptable use, consequences for unacceptable use, and basic rules that your school has regarding using the computers. Usually to make sure you read it your school wants both you and your parents to sign it.

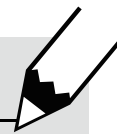
RULES, RULES, RULES!!!

Just like everything else, your school has rules for using the Internet. These rules are necessary to ensure that you are using it appropriately for school projects such as research and online field trips. Your school's AUP should cover what would happen to any student who uses the Internet inappropriately at school. Do you know your schools rules and consequences regarding Internet Use? If not, it's time to find out!

BRAINSTORM:

Name a few things you think your school's AUP policy should cover?

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____



LESSON—Cyber Bullying

Suggested grade levels 7-8

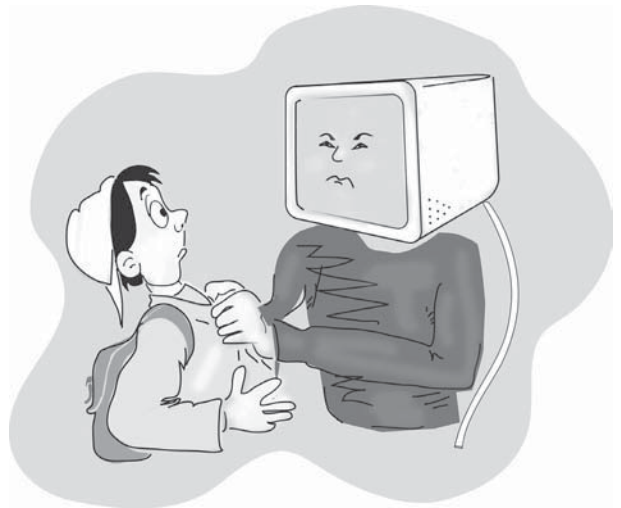
Lesson Guide

Students will become more familiar with online communication and consequences of cyber bullying.

Learning Objectives

Students will:

- develop an understanding of the following terms and definitions:
 - > **e-mail**: electronic mail
 - > **flame mail**: mail intended to make someone angry or hurt
 - > **hate mail**: mail that shows racism, sexism, or other prejudices
 - > **cyber bullying**: online harassment or degradation
- be able to identify online bullying, prevent bullying, and find help if victimized



Materials

- a copy of the reference page for each student
- a copy of the parent page for each student

Procedures

Discussion

- Introduce students to the concept of an online cyber community. Ask students what the benefits of an online community are.
- Ask students to think of some negative sides of an online community. Lead into informing students that they will address one negative aspect that can occur online—cyber harassment.
- Ask students to define a bully. Discuss their ideas. Provide students with the following definition of bullying: Bullying consists of ongoing threats, physical attacks, words, gestures, or social exclusion directed at a student or students by a student or group of students who are older, bigger, or more powerful. Discuss with students how bullying can occur while online.

Reference Review

- Divide students into small groups, and hand out reference sheets on cyber harassment.
- Students should read and discuss the information on cyber bullying in their small groups.

Scenario/Skit Writing

Using what students have learned from their group work, have them write a scenario or skit on cyber bullying. Students will then present their short skits to the class.

After having students read the overview information in their groups, explain their task to them.

1. Students should brainstorm on the topic of cyber bullying based on what they know, what they have experienced, and what their peer group has experienced.
2. Students should write a scenario/skit identifying the issue and how to resolve it for the scenario they have chosen.

Skit Presentations and Discussions

- Students should present their short skits to the class.
- Discuss the skits and what students have learned about cyber harassment/bullying as a class.



Help students find ways to share their skits outside of the classroom with other classes, faculty, parents, etc.

Children who participate in activities and share what they have learned about Internet safety are more likely to practice safe habits online.

Additional materials and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. E-mail international@isafe.org for more information.

REFERENCE—Cyber Bullying Fact Sheet

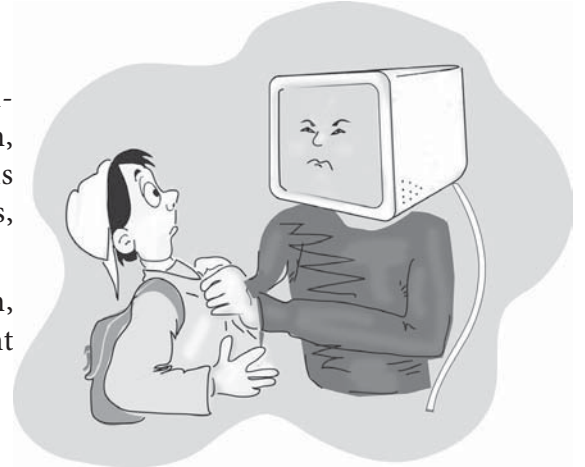
Suggested grade levels 7-8

Bullying has become an online, as well as a physical, event. Intimidation online can be just as bad, and in some cases even worse, as bullying that occurs in the physical community.

What is Cyber Bullying?

Cyber bullying is a threat that many youth face these days. Unlike the schoolyard bully who relies on physical intimidation, a cyber bully uses words and images to break down a victim. This harassment can occur in e-mail, text messages, instant messages, and chat rooms, or on Web sites.

Many youth consider cyber bullying as bad as, or worse than, physical bullying because it can occur 24/7. Unrelenting torment can drive a victim to drastic action.



What Can Be Done?

- As obvious as it may seem, if you are bullied, ignore it, or tell a trusted adult. And if you are tempted to bully someone else, don't! Many youth fall into the trap of not thinking about the consequences of unkind messages sent via the Internet because they can't see the person they are hurting.
- Reread messages, and make sure they can't be taken the wrong way. Sometimes things are taken out of context or meant as a joke, but the recipient doesn't realize this and is hurt.
- Use emoticons to help show what you really mean in your messages.
- Most importantly, stand up to others who bully online, and be a good cyber citizen! Remember: Being a bully online shows you aren't confident in yourself—you're resorting to making someone else feel bad to make yourself feel better.

Don't Be A Victim

1. Get Help! Find an adult who will listen and take you seriously. Unfortunately, this doesn't always happen with the first person you tell. You may have to tell several adults until you find one who will take action. Just remember: Cyber bullying is WRONG—you are RIGHT to get help.
2. Don't open, view, or respond to cyber harassment. It is beneath you to pay attention to it! Most likely they are bullying you to make themselves feel better.
3. Stay protected—never agree to meet with anyone you meet online.
4. Different situations can be resolved in different ways. An adult can help you find the best solution, whether it be contacting police, having the school take action, etc.

Remember: Getting help is a sign that you are a strong, confident person who will stand up for him or herself by getting help! You should never feel ashamed to take steps to make your life, or the life of a friend, better.

Prevention Techniques: How to Keep From Being Bullied Online

- Don't give out personal information, such as passwords, PINs, name, address, phone number, school name, or family and friends' names. This information can be used by bullies and others to harm you on the Internet.
- Don't exchange pictures or give out e-mail addresses to people you meet on the Internet.
- Ask permission from parents before you give out personal information online.
- Don't send a message when you're angry—it's hard to undo things that are said in anger.
- Delete messages from people you don't know, or those from people who seem angry or mean.
- When something doesn't seem right, it probably isn't. Get out of the site, chat, etc.

WILLING PARTICIPANT

i-SAFE Lesson Plan

Suggested Grade Level – Middle School

Learning Objectives

Students will:

- understand the concept of willing participation
- understand the safety risks of pursuing online relationships/friendships

Enrichment Goal

i-SAFE enrichment activities are designed to be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at www.isafe.org.

Learners will create a poster or bulletin board to inform others about strangers on the Internet and to provide strategies to stay safe in online communication.

Materials/Preparation

- a copy of survey page for each student
- materials to make a poster or bulletin board

Note: This lesson can be enhanced with the optional “Pool Party” video clip (.wmv format) located in the Downloads section of the Grades 6-8 CD or on the Curriculum Video Clips CD, available for purchase at <http://auth.isafe.org/store/>

Pre-Assessment

If beginning the i-SAFE program with this lesson, administer the pre-assessment online at www.isafe.org by clicking on “Assessments” prior to the lesson. To verify school ID number, log in at www.isafe.org, go to the “My Info” page, and select “Find Your School ID.”

Lesson Procedures

All students participating in the i-SAFE curriculum are considered i-MENTORs. If they haven't done so already, have students enroll online by clicking on “Create Account” at www.isafe.org to take full advantage of the support and incentives offered. This may be done at any time during the lessons, or students may complete this registration at home. If you would like to register your students yourself, simply go to <http://www.isafe.org/teachermentorprogram> and fill out the information for your students; then e-mail to outreach@isafe.org. Your students will then be enrolled, will receive information about sharing Internet safety with other students, and will be registered to participate in contests to win prizes.

Introductory Activity: Survey

- Pass out the survey to students.
- Have students complete the survey according to directions provided.

Survey Discussion

1. Why do you go online?

-
- Discuss with students that many students go online to meet people, socialize, etc. The Internet is a great way to correspond, etc. In fact, at some point, they may have had pen pals online at school. The key to having safe online relationships is to avoid revealing personal information and to keep an adult informed about the relationship.
2. Would you chat with someone with similar interests if they were:
 - Discuss the concept of willing participation. Many find nothing wrong with sharing online interests and creating friendships with someone older online. This can be the beginning of a “willing participant relationship,” in which the friendship could progress into a more personal or intimate relationship. It is important to remember that any type of personal relationship with someone older is inappropriate. Let your parents guide you in your online relationships.
 3. How do you determine the age of people online?
 - Reinforce to students that it is not always possible to determine how old someone is online. It is easy for people to lie online. Because you are behind a computer screen, you cannot perceive deception easily.
 4. Would you hide an online friendship from others?
 - Explain to students that helpful and beneficial relationships are never secret. Secrecy is the key ingredient of an inappropriate relationship.
 5. Do you add people to your buddy list when online?
 - Remind students that those people added to a buddy list when online are still strangers—you have never physically met them, and they should be treated with caution. Encourage students to only add those people to their buddy list who parents approve.
 6. Do you “personally know” everyone on your buddy list?
 - Tie into above question. Those on buddy list who are not “known” are strangers.
 7. When does being friends with someone online become “inappropriate”?
 - Secrecy, intimacy, etc., are all signs of an inappropriate relationship. Online relationships NEED to be discussed with an adult. Sometimes when we form online friendships, we lose objectivity and could be entering danger zones. Our parents can help us make careful and wise decisions.
 8. Do you know of any friends with online relationships that they keep secret?
 - It is important to share this information with a trusted adult. Online relationships can skew judgment, and your friend could potentially be in danger.

OPTION: Play *Pool Party* video

Read Article

Read the resource article about Katie Tarbox, found at the end of this lesson plan, to the class.

Discussion

Pass out the reference page on willing participation, and have students go over it as a group. Discuss the story:

- List possible reasons why Katie considered Mark a trustworthy friend.
- List ways that Mark “groomed” Katie to be his victim.

-
- What are possible reasons why Katie continued to enter Mark's room even though she felt uncomfortable about it?
 - What are possible reasons that Katie had a hard time making the decision to have Frank prosecuted?
 - Why do we call Katie a willing participant in the relationship? How can similar mistakes be prevented?

Concluding Discussion

As a class, discuss the following:

- Remind students that anyone met online is a stranger. As such we can not know their motives in pursuing an online relationship.
- If you feel it necessary to pursue online friendships, involve your parents and discuss these relationships with them.
- Remember that SECRECY is a sign of an inappropriate relationship.

Enrichment Activity

Youth who participate in activities to share what they have learned about Internet safety are more likely to practice safe habits online.
Additional lessons and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. at www.isafe.org.

Have students create a poster or bulletin board to inform others about strangers on the Internet and to provide strategies to stay safe in online communication.

Post-Assessment

Administer the post-assessment online at www.isafe.org by clicking on "Assessments" if this is your last lesson for i-SAFE. To verify school ID number, log in at www.isafe.org, go to the "My Info" page, and select "Find Your School ID."

Related Lessons

The i-SAFE lesson "Privacy and the Internet" (webcast) provides additional related information.

Contact us

We'd like to hear from you! E-mail teachers@isafe.org to share any unique ideas and/or experiences you had during implementation of this lesson.

The Katie Tarbox Story

13-year-old Katie began using a computer, the Internet, and chat rooms, aware of only the excitement, not the danger, in connecting with millions of others. One Sunday morning in a teen chat room, she met a guy named Mark who said he was 23 and a college student. Although Katie recognized the difference in their ages, she thought their conversation harmless. It was just the Internet. She felt very safe behind the computer screen. Katie thought of herself as too smart and too clever to become a victim. She was a high honors student, a national swimmer, and a very accomplished musician.

Katie and Mark had an amazing connection. They liked the same music, clothing styles, movies, and food. During a six-month period, they developed a friendship Katie characterized as “platonic, but important.” She could tell him anything and did. She discussed school, her family, her friends—and he always understood. But he wanted to meet her. Her parents knew nothing about the friendship, so it was not an option for him to visit her in Connecticut, and she would not be allowed to travel to California alone. Katie and Mark came up with a plan about Texas. She would be there with her swim team for a swim meet, and her mom would be along as a chaperone. It was perfect.

Katie shared her secret plans with her best friend as they arrived in Texas. She was going to meet her cyber friend! When the time came to meet and Mark opened the hotel room door, Katie did not feel quite as confident. She immediately noticed that Mark looked older than 23, but this was the person she had come to know so well. Although she felt uncomfortable about it, Katie entered the room. When he began molesting her, she did not know what to do. Fortunately, Katie’s friend from the swim team did not keep her secret. Katie’s mom and the hotel security arrived in the nick of time to rescue her.

Katie was shocked to learn that Mark was not Mark at all, but Frank Kufrovich, a 41-year-old financial analyst with a sordid past. Frank was an Internet predator. He had committed other crimes against numerous young girls and one boy. Going to trial was a big decision for Katie. Although it was a very difficult choice, she knew that if she went through with it and testified against Frank, other kids and teens would be safer on the Internet. Because of Katie, Frank was prosecuted in court and was sentenced to prison.

Katie still deals emotionally with what happened. It has left a lasting impression on her. She learned the hard way that people are not always who they say they are on the Internet.

Resource: Katie.com: My Story by Katherine Tarbox. Dutton Publishing 2002.

Willing Participant

It's fun to meet and communicate with people on the Internet. And most of the time online friendships can be great when they stay ONLINE! When you engage in an online friendship with a stranger, you are considered a "willing participant."

Be aware: It takes constant attention to detail to maintain a SAFE online friendship.

Here's why:

The anonymity of the Internet means that trust and intimacy can develop quickly. It becomes easy for one to forget that this is communication with a STRANGER. It becomes more difficult to avoid revealing personal information.

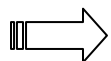
Finding Out About You Through . . .

Indirect Information

"Indirect" information includes details about you and/or your activities that are not always considered personal information. Bits of indirect information can be pieced together to identify how to find you.

Examples of indirect information are:

- your sports team number
- your team name
- a school event
- the date of a concert you will be attending
- the name of a shopping center that is near your home



Think of other things that could be indirect information about you.

Indirect information is usually given up during normal conversation. It is often hard to realize that you have given up so much information.

Remember: Indirect information can be gathered over a period of time to be pieced together.

What can you do about it? Be aware of what you say online and who you are saying it to at all times.

Survey

Directions: The following survey is anonymous and is for your own use as a reference for the class discussion. Answers will be used for discussion purposes only and will not be used to provide anyone with personal information about your Internet use.

Select the answer that applies to you. If more than one applies, select all that apply.

1. Why do you go online?

- a) to make friends
- b) do homework
- c) play games
- d) communicate with existing friends.

2. Would you chat with someone with similar interests if they were:

- a) your age
- b) in their 20's
- c) Much older than you (30+)
- d) younger than you

3. How do you determine the age of people online?

- a) they tell you
- b) you can tell from things they say
- c) age doesn't matter online
- d) you stick to teen areas when online

4. Would you hide an online friendship from others?

- a) Yes
- b) No
- c) Depends on circumstances

5. Do you add people to your buddy list when online?

- a) Yes
- b) No

6. Do you "personally know" (from the real world) everyone on your buddy list?

- a) Yes
- b) No

7. When does being friends with someone online become "inappropriate"?

- a) if they want more than friendship
- b) if they ask to meet you in person
- c) if they ask for personal info
- d) never, if you ask parents permission/keep them involved

8. Do you know of any friends with online relationships that they keep secret?

- a) Yes
- b) No

Negative Networking: A Look at Gangs Online

i-SAFE Lesson Plan

Suggested Grade Level – Middle School

Learning Objectives

Learners will:

- identify ways online communities can be used in negative ways
- become familiar with the negative ways the Internet is being used to network gangs and gang activity
- identify online services designed to counteract negative online activity
- discuss how online gang interaction can help authorities
- identify online gang activity that needs to be reported to authorities immediately
- know who to report online gang activity to

Enrichment Goal

i-SAFE enrichment activities are designed so that they can be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at www.isafe.org, including the i-Mentor Training Network videos.

In this lesson learners will be provided with background information to create a poster or flyer awareness campaign to promote safe online interaction.

Materials / Preparation

- online access to the i-SAFE assessments, if appropriate for this lesson
- copies of the reference pages for each student
- student registration in mentor program at www.isafe.org

If beginning the i-SAFE program with this lesson, administer the pre assessment online at www.isafe.org by clicking on the link, Assessments, prior to the lesson. To verify School ID#, login at isafe.org, go to the “My Info” page and select “Find your school ID”.

Lesson Procedures

All students participating in the i-SAFE curriculum are considered to be mentors. If they haven't done so already, have students enroll online by clicking on “Create Account” at www.isafe.org to take full advantage of the support and incentives offered. This may be done at any time during the lessons, or students may complete this registration at home. If you would like to register your students yourself simply go to <http://www.isafe.org/teachermentorprogram> and fill out the information for your students and email to outreach@isafe.org. Your students will then be enrolled to receive information about sharing internet safety with other students and will be registered to participate in contests to win prizes.

Discussion 1

- Review with students what the cyber community is:
 - Why is the Internet considered a community?
 - How is it similar to the physical community? How is it different?
 - What are benefits and dangers of this online community?
- Ask students how online communities can be used in negative ways? *Examples: online gangs, cyber bullying, predation, etc.*
- Explain to students that today they will be looking at one way negative networking occurs – the use of the Internet by gangs.

Reference Sheet

- Hand out the reference page to the students and read the first page, “Negative Networking”, as a class.
- Use the second page, “Food for Thought”, to discuss the following:
 - What types of things would some people do if they thought they could not be found out online?
 - What types of things do people do to gain friends and a sense of identity?
 - What possible uses would gangs have for the online environment?
 - How does online gang interaction actually help authorities?
 - If you see online gang action, symbols, etc, who should you report it to in your school or community?
 - How can reporting online gang activity and other types of online activity representing threats, plans, etc. help create a safer community and school environment?

Class Activity – Create a Reporting List

Reinforce to students that it takes a **team effort** involving school, community, and police partnerships to meet gang related challenges.

- Brainstorm a list of possible people/organizations that students can report online gang information to.
- Identify that law enforcement personnel (police) **MUST** be called in to prevent victimization related gang activity, online or offline.

Activity

- Divide class into small groups.
- Pass out materials to design posters.
- Use the information on the reference page and the list you have created in class to have students design posters or flyers with information on how to report online gang action or other dangerous activity publicized on the Internet to community or school officials.

Enrichment Activity

Youth who participate in activities to share what they have learned about Internet safety are more likely to practice safe habits online.
Additional lessons and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. www.isafe.org.

Complete the poster/flyer awareness campaign by posting and/or distributing the information around the school or at school events.

Notify i-SAFE about your students' activities by email to outreach@isafe.org.

Post Assessment

Administer the post assessment online at www.isafe.org by clicking on the link, Assessments, if this is your last lesson for i-SAFE. To verify School ID#, login at www.isafe.org, go to the “My Info” page and select “Find your school ID”.

Related Lessons

The i-SAFE lessons on Social Networking and Cyber Bullying provide additional related information.

Contact us

- We'd like to hear from you! E-mail teachers@isafe.org to share any unique ideas and/or experiences you had during implementation of this lesson.

Negative Networking

Predators are not the only ones to make use of the Internet's social networking capabilities for illegal or unethical purposes. Many other groups have also started making use of these networking communities for reasons that are a little darker and inappropriate.

The Anonymous Factor

Many people have written about how the Internet and its perceived anonymity leads to a lack of inhibition in people. Feeling that their real world identity is hidden, people feel free to do and say things they may not in real life. Notice this is a perceived anonymity – no one is truly anonymous when online – A fact that is important to remember.

However, it is important to also remember that no one person wants to be completely anonymous. That would be like being invisible. Instead a person uses the Internet to pick and choose the facets of their personality they want to express. In addition, some people join communities otherwise known as gangs to help represent and express their identity and to keep from being anonymous.

Gangs Online – Digital Graffiti

Gang members want and need attention and publicity. Street gangs have taken their fight online – creating websites to display their colors, gang symbols, and to warn their enemies. According to gang experts, these sites serve a similar purpose to the graffiti tagging that gangs have done for years. These sites serve to bolster egos.

It is important to know that online gang sites may not necessarily be run by true street gangs. Many are created by past members, bored teens, etc. Those that are run by true gangs DO NOT necessarily recruit members since membership is about loyalty, trust, and friendship – things they feel cannot be proven online. Instead what these sites do is promote the “cool” factor of gangs.

For example one gang site features pictures of bull dogs, women, expensive cars and more trying to glamorize the life. Additionally some sites have forums for gang members to give props (respect) or disses (disrespect) to other members.

Meanwhile law enforcement actually appreciates websites by gang members because it helps to confirm information and allows them to keep an eye on the gang. Information found on gang websites such as pictures and postings has lead to longer jail sentences for gang members convicted of crimes.

Some Internet Gang terminology:

Use of the internet and online sites for gang activity is known as *Netbanging*.

Snitches is a term used to identify those who tell on gang activity. However, gang use of the Internet has resulted in a type of self snitching as cops monitor websites.

The important thing to remember – not all of this online activity is just kids looking for thrills. Some of it is active gang members using web sites to communicate with each other, pick fights with rival gangs, schedule hits, and more. These sites should be avoided for several important reasons: 1) you do not want to get caught up in illegal activity 2) these sites can get dangerous 3) police do monitor these sites and use them as evidence in court. So stay safe online and stay away from negative networking sites!

Bully Boards

Gangs aren't the only online negative networking going on. Whole boards are popping up dedicated to allowing users to mock, bully, hurt, and degrade others. These sites promote gossip and negativity in their users. Why would anyone feel they need to attack others online? The common answer is to make themselves feel better. Just remember – don't sink to that level.

Team Effort

It takes a team effort involving school, community, and police partnerships to meet gang related challenges. You are an important part of that team!

- Police **MUST** be called in to prevent victimization related gang activity, online or offline.
- Use your time today to identify where to call to report in your area.



Promoting Positive Networking

Discuss the following:

- What types of things do people do to gain friends and a sense of identity?
- What possible uses would gangs have for the online environment?
- How does online gang interaction actually help authorities?
- If you see online gang action, symbols, etc, who should you report it to in your school or community?
- How can reporting online gang activity and other types of online activity representing threats, plans, etc. help create a safer community and school environment?

Positive Online Help

Some people have seen a need for those youth who may be struggling with identity problems and/or who may have had negative gang experiences. They have developed organizations that use Internet websites to provide guidance, resources, and help services to youth in need. One such site reported that almost half of its 345,000 “hits” in a six-month period were made by active gang members.

Discuss how this type of online activity adds positively to the cyber and physical communities.

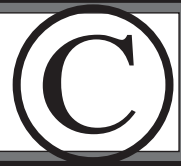
How can you help?

Use the results of your discussions to brainstorm ways to inform others about promoting positive online networking. Use the information you have learned about reporting gang incidents or online activity. Include information your school endorses about how to report information found online that indicates a threat to local students.

Create flyers or posters to spread your message!

LESSON PLAN—Intellectual Property and Copyright

Recommended learning level: Middle School



Learning Objectives

Students will:

- recognize the copyright notice and its meaning
- age-appropriately understand how copyright laws apply to creative works of authorship
- be able to demonstrate their knowledge and understanding of copyright protections



Materials

- a copy of the reference page for each student
- a copy of the activity page for each student
- access to a blank board or chart



Procedures Discussion

- Guide a brief discussion about property and lead into a definition of intellectual property.
- Ask students what they consider to be property. Discuss their answers and list them on the board.
- Ask students if something one of them thinks up, and then writes, draws, or makes, is property. Ask how this is different from regular property.
- Discuss why these items should be considered property. Ensure that the following points are covered: many people make their living from them, they belong to, or are owned by, the creator.



Reference Page and Continued Discussion

- Pass out reference page and have students read it over. Refer to the section on copyright in the Teacher's Guide, to add information that is age appropriate for your students. Continue the discussion with the following topics:
 - > What does copyright mean? Copyright is protection provided by the laws of the United States to the creators of things like books or other written works, as well as other dramatic, musical, and artistic works. To be protected by copyright, the works must be in tangible form. This protection means that the owner has control of what can be done with his or her original work.
 - > Copyrighted works are protected from being copied, distributed, performed, or changed without the creator's (or owner's) permission. This protection is available to both published and unpublished works, and applies to students' work.
 - > What does the term intellectual property mean? Intellectual property is a product of the intellect, such as inventions, music, written word, and pictures.
- Have the class brainstorm examples of intellectual property that they think have some type of value to the creator or owner.
- Possible examples: music you hear on the radio makes money for its owners; an author makes money from his books; a school project made by a student may get a good grade.

- Discuss the scenario about the teacher using his student's work. (The essay is intellectual property that belongs to the student. The teacher should have obtained permission from the student before posting.)



Group activity

- Divide students into small groups and provide each group with an activity page.
- Instruct students to complete the first section. They should consider the work, money, effort, etc. that goes into creating work that is protected by copyright. Discuss if desired.
- Have students complete the chart using the information they have learned in this lesson.

Presentation

- If desired, prepare a section of the board or a large chart to record answers.
- Have the groups take turns sharing the points they included on their charts.

The charts should include the following information:

Protections:

- Copyrighted works cannot be copied without permission (given).
- Copyrighted works cannot be distributed without permission.
- Copyrighted works cannot be performed without permission.
- Copyrighted works cannot be changed without permission.

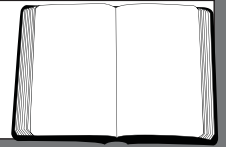
Results of Protections:

- Enables an artist to become known for his/her work (given).
- Is an incentive for the creation and production of more creative works.
- Enables the creator to make money from his/her work.
- Gives the creator legal foundation in a court of law to protect his/her work.

Evaluation

- Review posters and/or webpages for concepts listed above.
- Acknowledge those who show the copyright notice on their work.

Copyright Know-How



As citizens, we have rights. A very important right is to be able to own property, and therefore, be able to say what is done with our property. Many times we think of “property” as something like land, a bicycle, or a soccer ball, but you have learned that intellectual property is a kind of property made from things that we can create using our minds. Each person who has created intellectual property owns it and has the right to say what is done with it. It’s called “copyright.”

The following kinds of intellectual property are covered by copyright:

literary works (books, stories, poems, etc.)
musical works including any song words
drama – plays and musicals
dances, ballets
graphic art such as paintings, drawings, digital art
photographs

sculptures
movies and videos
radio and television broadcasts
sound (audio) recordings
designs for buildings
computer software



Copyrighted works are protected from being copied, distributed, performed, or changed without the creator’s (or owner’s) permission. This protection is available to both published and unpublished works.

It is important for people to let others know that their own work is special and deserves the respect of copyright. This is done by putting a special notice on the work made up of the copyright symbol – a letter “c” inside a circle: ©, the year, and the name of the creator.

Copyrights begin upon creation of a work in tangible form (a form that can be seen or touched).

Although copyright registration is not required, registration of a copyright with the U.S. Copyright Office creates a legal, public record of the copyright facts and details. This is especially useful for materials that have known commercial value. Go to <http://www.loc.gov/copyright> for instructions on how to register copyright.

Think About It – Talk About It

You have written a long essay as an assigned school project and you turn it in.

Your teacher thinks you deserve an A and without telling you, he proceeds to post the text of it on an online bulletin board to show other teachers the work his students are doing.

- Was it legal for the teacher to do that?
- Do the laws of copyright apply here?
- Is this fair? To whom, and why?

Why Copyright?

A lot about copyright is about money! If people are allowed to have copyrights and make money from them, it is a strong incentive for the creation and production of creative works. Copyright provides a measure of control over one’s creations. In order for someone to bring a lawsuit against another for copyright violations, the creative work must have commercial (monetary) value.

The Value of Copyright



If you create a work of art such as a story, a song, a painting or a photograph, what is your investment (effort, time, money, etc.)?

Choose a type of work that would be protected by copyright, and that you might create (a story, song, painting, etc.) and fill in the following:

Materials you would need:

Cost of those materials:

Time to create:

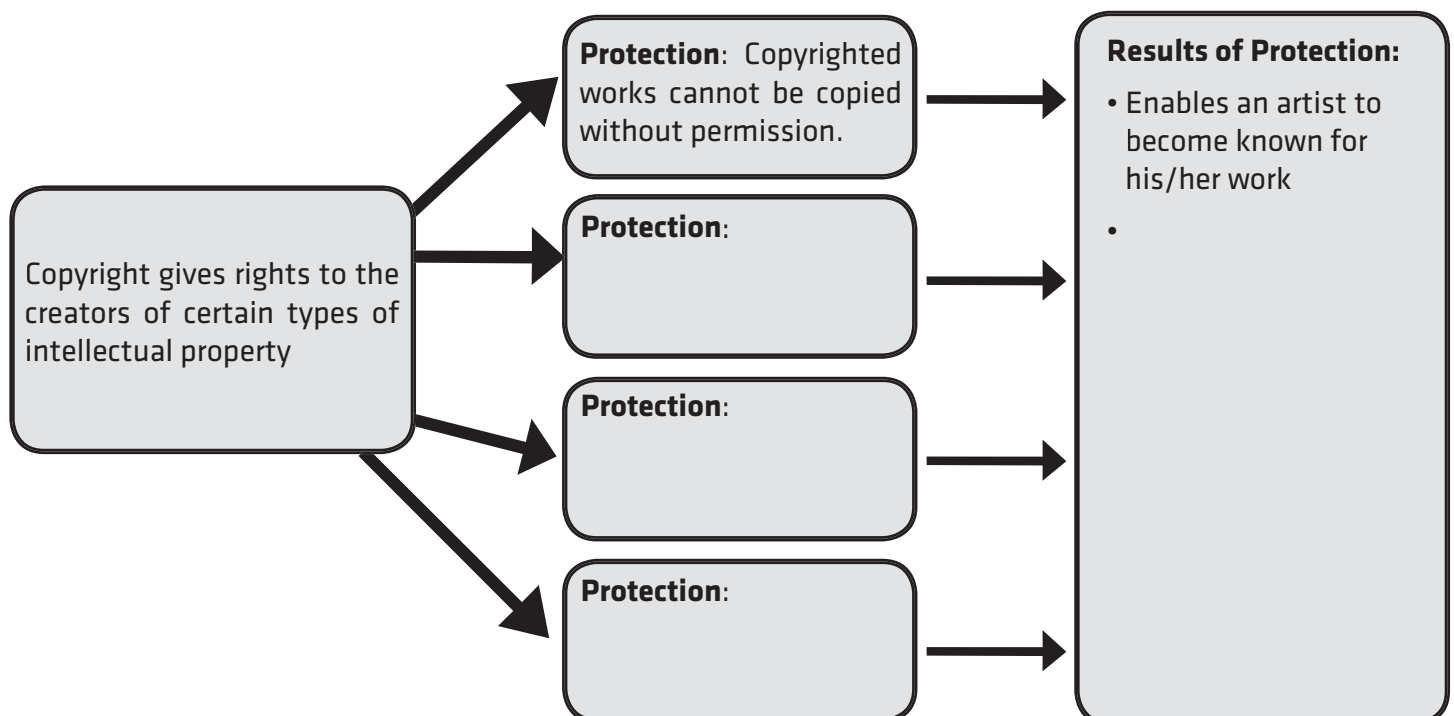
Cost of your time:

Distribution – how would you distribute story? Cost/Time factor:

What would be the impact of someone taking your story, copying your story, or stealing your story?

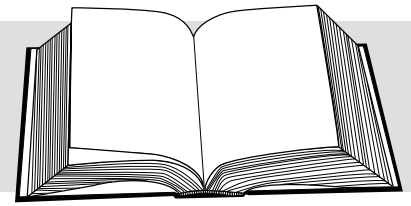
Chart it!

Directions: Using the reference information from this lesson and the chart below, organize your thoughts on the reasons copyright protection for original works of authorship is as important as the laws that protect ownership of other tangible property. Some boxes have been filled in to help you get started. When finished, create a small poster or webpage with your group, to let others know about the importance of copyright protections.



A Web 2.0 World

Unit Overview



Suggested grade levels 6-12

This is a comprehensive unit, inclusive of resources, a lesson plan and sets of activities, designed to enable student and instructor understanding of Web 2.0 terminology and the founding technological activities that gave rise to the concept. In this unit, i-SAFE utilizes its traditional format of enabling learners to use critical-thinking skills to construct knowledge and develop positive concepts, by using articles on the pros and cons of Web 2.0 usage in the classroom in a variety of activity options.

Unit Content

- Understanding Web 2.0 (resource article)
- Web 2.0 Terminology Guide
- Web 2.0 Lesson Plan
- Pro and Con Web 2.0 articles for debate activity
- Suggested coordinating activities to utilize the concepts learned



Unit Goals

Students will

- develop an understanding of the terminology associated with the Web 2.0 world
- understand how the Web 2.0 world arose
- examine how Web 2.0 technology affects the educational world
- understand the safety and security risks of Web 2.0 technologies
- propose meaningful integration of Web 2.0 technologies into the school climate



Enrichment Goal

i-SAFE enrichment activities are designed to be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at **www.isafe.org**. Completion of this unit will prepare and guide learners to utilize Web 2.0 technologies to spread the message of e-Safety to others.

Preparation

- Provide online access to the i-SAFE assessments, if appropriate for this lesson.
- Read through the lesson plan and select from the suggested activities.
- Make copies of the appropriate reference and activity pages for each student.
- Enable computer access for enrichment activity completion.



Pre-Assessment

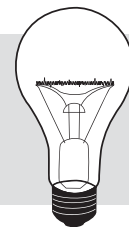
- If beginning the i-SAFE program with any lesson in this unit, administer the pre-assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID."

Post-Assessment

- If ending the i-SAFE program with any lesson in this unit, administer the post-assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID."

Understanding Web 2.0

Resource Article



Have you heard the term “Web 2.0” used and not quite understood what it meant? Perhaps you have wondered, is this new software or hardware, or perhaps a new Internet? Something else I have to learn? Or, perhaps you’re one of those who is leading the way and have been utilizing Web 2.0 technologies for years.

So just what is Web 2.0? Although the term suggests a new version of the World Wide Web, it is actually used to refer to a new way of utilizing Web technology to facilitate creativity, collaboration and inter-user cooperation. This new world arose as Web-based communities and services such as blogs, wikis, social-networking sites, user-created video sharing, and more gained prominence.



The term developed to suggest improvement over the “old” version of the flat, non-interactive Web which was primarily comprised of users visiting read-only Web sites. To the new way of thinking, these types of sites are out. Instead, Web site focus is on interactivity, or allowing the user/viewer to interact rather than being a passive receiver.

Web 2.0 theory is about an “architecture of participation,” a term coined by Tim O’Reilly in 2004. Think about that quote. How can the online environment foster such participation? The answer is by allowing visitors to have a stake in content through their own interaction. In a way, the evolution of the Internet has mirrored the evolution of education. At one point it was believed students were passive vessels waiting to be filled by a teacher who could lecture or instruct: teacher-centered. This learning concept has been proven by research to be ineffective. Therefore, learner-centered education has become the focus, allowing learners a stake in their education through engaging activities, discussion, self-directed learning and processes that allow a scaffolding of knowledge. It results in a more engaging and rewarding experience. Obviously, this also applies to online interaction.

It is likely that even if you are not aware of the actual terms of Web 2.0, you are already using technologies that facilitate it. Many of the ways you choose to interact online are the basis for Web 2.0 terminology. Blogging, adding to a wiki, interacting on a social network, and virtual worlds, are all examples of the way the online world allows for the rich interaction Web 2.0 users expect.

If the history of the Internet so far is an indication of the future, it is likely that the term Web 2.0 will also become passé, overwritten as others have been by technology that is always changing and progressing. The important goal, however, is not to adopt new terminology, but to recognize that digital technologies, including the Internet, are becoming more interactive and user controlled.



- **Web 2.0** – A perceived second generation of Web services such as Web-based communities and other hosted services whose aim is to facilitate creativity, collaboration, and sharing between users. Well-known examples of successful sites that are founded on Web 2.0 interactivity include Google, Wikipedia, Flickr, Second Life, YouTube, Digg.com, MySpace, and Facebook.
- **Blog** – Web site with journal-style entries listed in reverse chronological order. A typical blog combines text, images, and links to other blogs, Web pages, and other media related to its topic. The ability for readers to leave comments in an interactive format is an important part of many blogs.
- **Wiki (Wikipedia)** – Wiki is software that permits users to create, edit, and link Web pages easily. Wikis are often used to form collaborative Web sites and to power community Web sites. Wikipedia is perhaps the best known wiki and is an arena for users to define topics.
- **Social Networking online** – Social networking online is built upon social networks that are set up for people who share interests, activities, or are interested in exploring the interests and activities of others while online. Most services are primarily Web based and provide a collection of various ways for users to interact: typically including chat, messaging, e-mail, video, voice chat, file sharing, blogging, discussion groups, etc.

- **Tagging** – Tagging is the process of creating labels for online content. It is a somewhat confusing term because there is debate about what should be officially counted as tagging. Some consider tagging to be no different than creating a traditional browser bookmark. Adding to the confusion of clearly defining the term, some sites invite users to apply “labels” to content and don’t use the word “tag.” Google’s tagging feature is actually called “bookmark,” although it applies the principles of tagging. Other sites enable tagging so effortlessly that people might not be conscious that they are doing it. According to the Pew Internet and American Life Project, 28% of online Americans have used the Internet to tag content, revolutionizing the way information is classified, enabling us to make better sense of it.

An example that can be used to illustrate the concept of tagging is Del.icio.us. (pronounced “delicious”), a social bookmarking web service for storing, sharing, and discovering web bookmarks. The site, founded by Joshua Schachter in late 2003, was acquired by Yahoo! in 2005. According to **www.wikipedia.com**, it has more than three million users and 100 million bookmarked URLs. It is interesting to note that on the Del.icio.us Web site, “tag” is defined as “... simply a word you use to describe a bookmark.”

- **Folksonomy** – A term that describes the function of Web sites that facilitate tagging. Folksonomy is also known as collaborative tagging, social classification, social indexing, and social tagging.

Another example that can be used to illustrate the concept of tagged file sharing, is **www.flickr.com**. After creating an account at flickr.com you can upload your photos to the site and then apply labels that you create to the photos. For example, if you upload a photo of a skateboarder and label it as “skateboarder,” anyone using Flickr’s search bar who types in “skateboarder” can find your photo among the other pictures that are similarly named.

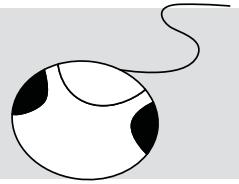
- **RSS (Really Simple Syndication)** – A family of Web feed formats used to publish frequently updated content such as blog entries, news headlines, or podcasts. An RSS document which is called a feed or channel contains either a summary of content or full text from an associated Web site. RSS makes it possible for people to keep up with favorite Web sites in an automated manner that’s easier than

checking them manually. Newer versions of operating systems automatically provide RSS feeds right onto your desktop or into your e-mail inbox.

- **Podcast** – A podcast is a collection of digital media files distributed over the Internet using syndication feed for playback on media players or personal computers. The term developed from the acronym pod, for portable on demand, and broadcast.
- **Virtual World** – A computer-based, simulated environment intended for its users to inhabit and interact via “avatar” identities. This habitation is represented in the form of two or three dimensional graphics. Most virtual worlds allow for multiple users. An example of a well-known virtual world is Second Life (www.secondlife.com).

Resource

Argument FOR (Pro) Educational Usage of Web 2.0



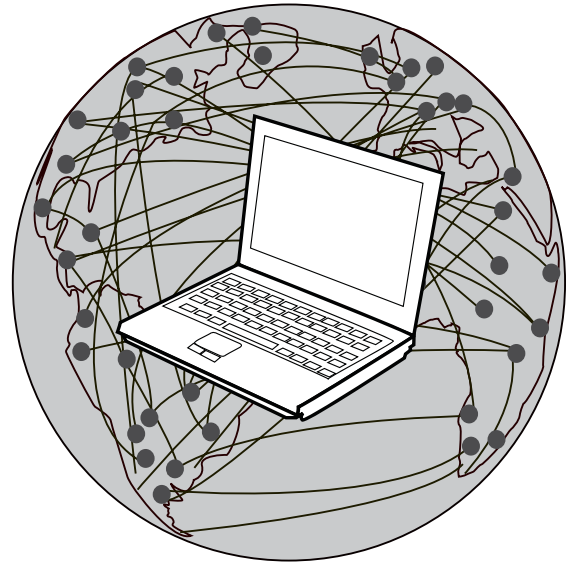
Think of technology as an ever changing and updating world. Part of the goal of our educational climate should be to ensure that students are graduating and moving into the workplace or on to college, familiar with the technologies they will be utilizing. Meeting this challenge requires that teachers be open to integrating new and emerging technologies into the curriculum. Today, this most assuredly includes Web 2.0 advancements.

In the past, the integration of computer usage into the classroom meant including a list of Web sites to visit and review, the use of basic online tutorial games and perhaps a simple online quiz. Little learner interaction or empowerment was involved.

Now, however, Web 2.0 is allowing educators to truly involve their students with the digital environment. Educators can utilize powerful tools such as blogs, media-sharing services and other social software. While these types of Web 2.0 advancements were not originally designed for classroom inclusion, they are easily adapted for a variety of assignments and activities, and provide excellent examples of real-life skills needed. Web services such as blogs, podcasts and even social networks, allow for the teacher to make online learning more personal, interactive, flexible, and empowering.

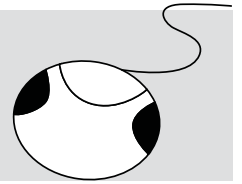
So how are forward-thinking educators actually utilizing Web 2.0 resources? Teachers are incorporating blogging into writing assignments, having class meetings in virtual worlds, allowing students to “become” characters from novels online, and more. A recent study published by Stanford University regarding the educational use of Teen Second Life found that by providing access to, and support for, educational opportunities in Teen Second Life, participants developed skills such as leadership, problem solving, teamwork, and communication – termed knowledge age skills – proving Web 2.0 can offer real educational benefits. To read the study view: <http://mediax.stanford.edu/seminars/schomeNAGTY.pdf>.

The sky is the limit with Web 2.0. Best of all, students are not only learning about the topic on hand, they are engaging in meaningful interaction and honing technology skills needed in today’s digital world. Younger children can learn while having fun and for those who are easily bored with school, participation in interactive online activities can be a great way to get them motivated to learn. Engaging in Web 2.0 activities at school allows students to learn in their technology comfort zone, and give them opportunities to demonstrate their technology skills and knowledge while developing other concepts.

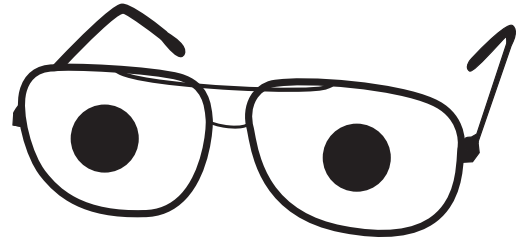


Resource

Argument AGAINST (Con) Educational Usage of Web 2.0



While there are definite possibilities to loosely relate Web 2.0 technologies to learning, the fact is there are better and more useful ways for students to learn material, with fewer risks. Furthermore, many students feel that adults/educators are encroaching on their turf when utilizing these technologies for educational purposes. After all, technologies termed Web 2.0 were not developed or intended for educational use.



Let's face it, any educator can stretch and make an assignment "educational." Take the example of a teacher who is doing a unit on the Holocaust. The teacher wants to show the movie, "Schindler's List." Is the movie educational? Yes. But many could argue that a student's time could be better used, such as reading a novel on the topic. Furthermore, many parents may reasonably object to the movie's content – not wanting their child exposed to the nudity and violence. The point is, just because an educator says something is educational does not mean it validates or justifies the time, energy and risk involved for students.

The same should hold true for online technologies. Getting students online is wonderful. Students need exposure to the online environment. However, do students really need to be blogging, posting projects on MySpace, or accessing Wikipedia as a resource for school projects? No! The little educational value the technology usage might hold in engaging in these activities does not outweigh the risks involved. Engaging in online interaction and communication leaves the student and school open to numerous risks from predators, to viruses, to the viewing of objectionable materials. That is why most filters block many of these types of sites. Additionally, Web content can be difficult to validate as anyone can post any information, true or not. Wikipedia is hardly a valid resource for research, and educators should instead encourage usage of online encyclopedias that have reputable, accepted print counterparts. Web 2.0 does not provide anything more educational than other, more traditional projects that have less risk.

Consider the recent study published by Stanford University regarding the educational use of Teen Second Life. Of note in the study was that many participants chose to spend little or no time online in this virtual environment. Few participants chose to log hours. It was necessary for students to spend time learning how to use the environment before they could actually participate. Furthermore, access problems caused by blocking by school firewalls gave them serious issues. Additionally, other problems such as grievers (online bullies) and issues of acceptable use were encountered. In light of these types of problems, it is difficult to see how any educational benefit could outweigh the problems.

Leave Web 2.0 to technology classes and allow the teachers to teach the material in their subject area in a safe and meaningful way. Teachers do not have the time to fully prepare lessons as it is, incorporating Web 2.0 is an additional time constraint with little benefit.

Lesson Plan – A Web 2.0 World

Procedures

1. Complete the first “All Students” section
2. Select and complete one of the Activity Options
3. Continue with the second “All Students” (enrichment) section

All Students Discussion

- Ask students if they have heard of the term, Web 2.0.
- Discuss what they think the term means.



Article

- Read the article, “Understanding Web 2.0” as a class.
- Ask students to create a concise definition in their own words for Web 2.0.
- Have students suggest examples of Web technologies that represent Web “1.0” vs “2.0.”

An example:

- Finding information using online encyclopedia vs. searching Wikipedia with user-created content
- Ask students if they know of any sites that have evolved to Web 2.0 – i.e., were flat/static sites and have become more user centered and interactive.

Select one of the following activity options to complete the lesson.

Activity Option 1

Debate Activity

- Read through the Debate Information and Guidelines and Debate Preparation Worksheet pages with students, and clarify the procedures you will follow.
- Students will either debate FOR incorporating Web 2.0 into the educational environment or AGAINST.
 - Pass out copies of the Pro and Con resource articles to the appropriate groups to be used either as a starting basis for their research or to generate ideas for their debate side.
- Provide time for students to research their position and to complete their worksheets.
- Allow students to debate the issue.
- Following the debate, have students vote – are they for or against inclusion of Web 2.0 in the school environment?

Activity Option 2

- Divide students into small groups.
- Pass out the T-Chart Diagram Handout.
- Have students brainstorm pros and cons of utilizing Web 2.0 within the classroom or educational environment.
- As a class, discuss why the educational environment might want to incorporate Web 2.0 technologies into the classroom. What are the benefits? What are the drawbacks? Are there risks?

Pro/Con Articles

- Hand out the pro/con articles to the groups and have students read through the two sides of incorporating Web 2.0 into the educational climate.
- Have them compare the two discussions to the charts they developed.

Activity Option 3

- Have students evaluate ways that your class or school already incorporates Web 2.0 technologies.
- Have students brainstorm class activities that could utilize Web 2.0 in a valid and meaningful manner.

All Students

Upon completion of the selected activity, proceed to the next section (enrichment activity).

Enrichment Activity

Directions

- Provide students with copies of the enrichment activity page, "Utilize Web 2.0 Theories."
- Students create a way to relay information on cyber security and safety utilizing Web 2.0 theories. Some examples include:
 - Creating a blog
 - Formulating a wiki entry
 - Creating an interactive site complete with links, area for comments, etc.

Documentation

- Please submit photographs of students who create exceptional youth-empowerment projects, for special recognition from i-SAFE. Photographs must be accompanied by corresponding personal a release forms.
- We'd like to hear from you! Send an e-mail to **teachers@isafe.org** to share any unique ideas and/or experiences you had during implementation of this lesson.

Children who participate in activities who share what they have learned about e-Safety are more likely to practice safe habits online.

Additional lessons and support for students to go peer-to-peer on e-Safety topics are available through **www.isafe.org**.

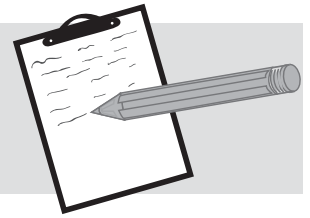
Post-Assessment

- If ending the i-SAFE program with any lesson in this unit, administer the post-assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID."

T-Chart

Advantages	Disadvantages

Debate Preparation Worksheet



TOPIC: _____

Opposition: _____ **Proponents:** _____

You are now a member of your selected team. Your success will be based upon the team as a whole. This means that you will be as strong as your weakest link. Be sure that you work together so that all members of your team have an adequate background of the positions and arguments that you will be proposing.

Only one team will “win” this debate. The winning team will:

- have a solid background regarding all material
- have plenty of evidence to back up claims
- use teamwork to teach all in group the important concepts behind specific positions
- be creative/psyche out opponents
- outclass opponents/never give an answer of “uh....”

Assign Roles:

1. Lead Presenter – Will be first to present constructive arguments of your side.
2. Second Presenter – Must present second side of arguments.
3. Lead Rebuttal – Must answer arguments by other side.
4. Final Rebuttal – Finish answering arguments by other side and offer summary/conclusion – wrap up arguments for your team.

Time to Prepare:

Define the Topic:

Make sure all terminology is clearly defined.

Define your Position:

Clearly state your position.

Arguments that Support Your Position

What are your arguments that support your position?

Preparation for Arguments Against Your Position

Be prepared! What will the other side argue? How can you rebut these arguments?

Summarize

Clearly summarize your arguments.

Tips:

- Do your research and check your facts. Are your sources biased?
- Have multiple sources.
- Make sure you can prove assertions. Don't just claim things – be prepared to explain and prove.
- Offer more than one argument. "Don't put all your eggs in one basket!"
- Be respectful.
- Listen carefully and take notes when other side is talking. Be prepared to answer their assertions.

Notes

Debate Information and Guidelines



Why Debate?

Debating forces one to prepare and learn all information available on a topic in order to present a concise and valid argument. Here are some great benefits of learning to debate:

- It's fun!
- Debaters become smarter –
 - Debate = analytical power = better job = job satisfaction, higher salary.
 - Debate = ability to communicate = happier friendships, family relationships, romantic relationships.
 - Debate = power to think = ability to improve things around you, have impact = satisfaction.
 - You get used to volume - juggling arguments. You get used to hard thinking. You get used to figuring out the weaknesses in others.

Debate Format:

For this lesson, the Team Policy Debate format will work best. It is designed for teams of 4 to debate on a topic with proper preparation.

A round of team policy debate consists of 8 speeches. The first 4 speeches are called constructive speeches, because the teams are perceived as laying out their most important arguments during these speeches. The last 4 speeches are called rebuttals, because the teams are expected to extend and apply arguments that have already been made, rather than make new arguments. Here is a table of the 8 speeches and their time limits:

Speech:	1AC	1NC	2AC	2NC	1NR	1AR	2NR	2AR
Time:	8 min.	8 min.	8 min.	8 min.	4 min.	4 min.	4 min.	4 min.

The teams are typically labeled as either being Affirmative or Negative. For example, in today's debate we will be debating whether Web 2.0 technologies are beneficial in education. First, that statement must be written as a statement of purpose or policy.

Web 2.0 technology is an important and valid method for inclusion in education.

Now, teams are either affirmative – or for this statement or negative – against this statement.

Team 1 will present an affirmative constructive argument. Team 2 will then present a negative constructive argument. This is repeated. Then, the negative team goes twice in a row with a negative rebuttal. A rebuttal is an argument that addresses the other team's arguments.

For the purpose of this debate, not only are preparation and research important, but also style and persuasiveness. Instead of using a traditional rubric for scoring points, the teacher and the class will decide the winner based on these means.

In addition to team roles, the teacher can assign the following roles:

Moderator (to maintain order and sequence of events)

Questioner (to clarify items by asking questions of teams)

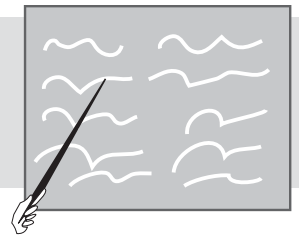
Time Keeper (monitors time of debates)

Things to Remember:

- Be polite – don't make personal attacks.
- Take notes during debate for rebuttal.
- Preparation is the key to success – KNOW YOUR TOPIC.
- Don't interrupt.
- Be confident – convince others you are right.

Utilize Web 2.0 Theories

Educate others about online safety and security



Ready

Think about what you've learned about safety and security in your class. How can you spread this message to others?

- Who is your audience? Adults, youth or both?
- What Web 2.0 technologies are you interested in?
- Collaborate with your group and sketch out how you will use Web 2.0 to convey your information.

Get Set

- Get creative and have fun using what you know about Web 2.0 – whether blogging, wikis, social networking, Web site design – the options are endless.

When you are finished –

- Make sure your information is educational and you have said exactly what you want to say.
- Ask a classmate or teacher to review it and offer constructive feedback.
- Make any needed corrections based on the feedback you receive.

Go!

- Go live online!
- Request permission to link your page, blog, wiki, etc., to the school's Web site, district site, and/or parent-teacher organization site so that others can benefit from your information.
- Inform i-SAFE – send a link to teachers@isafe.org.

LESSON—Online Social Networking—a New Way to Socialize

Suggested grade levels 9-12

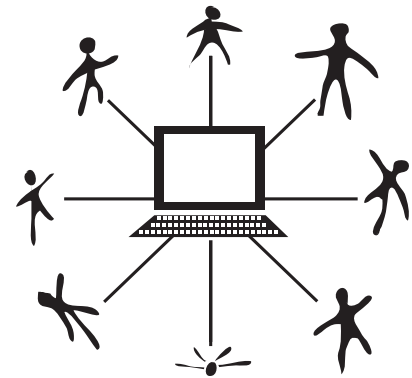
Lesson Guide

Learners will examine the risks and benefits associated with providing personal information through online social networking.

Learning Objectives

Students will:

- describe risks and dangers associated with online social networking
- create tips on how to minimize risk when using social-networking Web sites
- share information on safe online social networking with peers



Materials

- a copy of the reference page for each student
- materials or facilities for creating posters or web pages

Procedures

Note to teachers:

Social-networking Web sites typically integrate Web profiles, blogs, instant messaging, e-mail, music downloads, photo galleries, classified listings, events, groups, chat rooms, and user forums to enable users to socialize. The information provided in this lesson can also be adapted to focus on specific types of networking, such as blogging.

Facilitated Discussion

Use the attached reference page titled “A New Way to Socialize” to facilitate a discussion about online social networking. Have students give examples and discuss each section.

Peer-to-Peer Activity

Either individually or in small groups, have students use what they have learned about the risks involved in online social networking to create safety tips. Have students create posters or web pages to share their safety tips with other students.



Help students find ways to publish and/or post their social-networking safety projects from the peer-to-peer activity.

Children who participate in activities and share what they have learned about Internet safety are more likely to practice safe habits online.

Additional materials and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. E-mail international@isafe.org for more information.

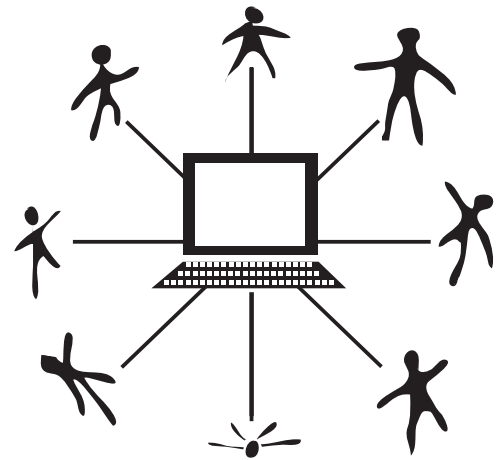
REFERENCE—A New Way to Socialize

Suggested grade levels 9-12

Guide to Social Networking

Social networking Web sites integrate Web profiles, blogs, instant messaging, e-mail, music downloads, photo galleries, classified listings, events, groups, chat rooms, and user forums to create connected communities where users publish details of their lives. Many people of all ages spend hours each day surfing and interacting on social networking Web sites. It is clear that online communities are changing the way people socialize.

In fact, statistics show that social-networking sites are among the most widely used global sites. Some sites rank in the top five Web domains according to numbers of page views.



Talk about it: Name social-networking sites popular in your area of the world. What are the benefits of socializing through online social networks?

Have you considered . . .

In addition to the positive aspects, social networking poses risks and dangers to users.

- Information posted publicly on a social-networking “space” can be viewed by anyone who logs on—friends, strangers, teachers, parents, parents of friends, etc.
- Cyber predators use social-networking sites to “groom” potential victims through the use of posted personal information and communication tools.
- Identity thieves prowl social-networking sites looking for victims to swindle.
- Information about you can be used by others to create a fake page or to bully.
- Comments online are in essence permanently recorded. Despite the casual and familiar feel of some networking sites, personal information is made available for people you may not approve of to copy, and it is sometimes impossible to have comments erased from public view online.

Talk about it: How might information obtained about an individual from a social-networking site be used in a negative way? How might information obtained about an individual from a social-networking site be used by a potential employer?

Dealing With Problems of Online Social Networking

Anyone who decides to participate in online social networking must consider all of the potential uses of posted information and take steps to ensure safe interaction.

- Review the site’s privacy policies.
Find out about it: How will information collected be used by the Web site owners?
- Review the site’s user guidelines.
Find out about it: Is there a code of conduct? Are there penalties for violators?
- Before creating a networking page, review and enable the privacy features, such as those that make your profile private and allow you to limit access to your space to people you actually know.
- Think before you post.
Think about it: You may later regret a comment or photo that cannot be deleted.

Legal Trends in Cyber Safety and Security

i-SAFE Lesson Plan

Suggested Grade Level – High School

Learning Objectives

Students will:

- be able to identify the ever-changing and evolving nature of laws as they pertain to the Internet, which is in its infancy
- be able to identify some of the current legislation/court actions regarding four main topics: cyber predators, cyber security, cyber bullying, and intellectual property
- be able to communicate to others their knowledge on legal trends of the Internet
- be able to take an active part in helping to form policy

Enrichment Goal

Learners will interact in the classroom environment through group discussion and examination of current legal trends as they apply to central cyber safety and security issues. Learners will be provided with materials to engage in an enrichment activity, which involves helping to form policy by writing to congressional leaders concerning the legal cyber security/safety issue of their choice. Ideas for further involvement in policy-making will also be given.

Materials/Preparation

- access to research materials
- a copy of reference and activity pages for each student
- materials as selected for the presentation portion of the lesson
- a congressional letter direction page
- online i-MENTOR registration (each student) to receive supporting i-MENTOR Toolkit materials

Pre-Assessment

If beginning the i-SAFE program with this lesson, administer the pre-assessment online at **www.isafe.org** by clicking on “Assessments” prior to the lesson. To verify school ID number, log in at **www.isafe.org**, go to the “My Info” page, and select “Find Your School ID.”

Lesson Procedures

Children who participate in activities and share what they have learned about Internet safety are more likely to practice safe habits online.

Additional lessons and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. at **www.isafe.org**.

Discussion

Direct a class discussion on the following:

- Ask students what types of issues and problems they face when online.
- Ask students what they know/understand on the following issues:
 - cyber predators
 - cyber bullying

-
- intellectual property
 - cyber security
 - Ask students if they know of or have school policy, state laws, or even federal laws concerning those topics.
 - Ask students if they have heard of any recent policy or legislation changes regarding Internet topics.
 - Present the idea that laws and policies regarding the Internet are constantly changing and evolving.

Peer-to-Peer (P2P) Activity

- Divide students into four groups.
- Assign each group a topic (cyber predators, cyber bullying, intellectual property, cyber security), and hand them that reference sheet.
- Student groups should read through and discuss the reference sheet they received.
- Students should create a mini presentation on the topic to educate the rest of the class.
- Have student groups present their mini presentation to the class.
- Discuss the legal trends mentioned in presentations.

Concluding Discussion

As a class, discuss the following:

- What legal trends were mentioned in the presentations?
- How are laws and policies regarding the Internet constantly changing? Why?
- What types of things would they, as students, like to see made into laws/policies?
- Lead into a discussion about the enrichment activity.

Enrichment Activity

Youth who participate in activities to share what they have learned about Internet safety are more likely to practice safe habits online.

Additional lessons and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. at **www.isafe.org**.

Inform students that they will write letters to their congressional leaders concerning an Internet safety or security issue, and discuss their ideas for legislation or policy regarding it.

- Pass out the congressional letter worksheet for students to fill out as you discuss getting started.
- Share with students the congressional letter information directions for getting started:
 - A congressional letter should be carefully written, edited, and revised. Make sure to follow basic formal letter-writing standards. Clearly state the problem as you see it, and offer suggestions for ways to solve this problem through legislation or policy changes.
- Have students research their state representatives and make a note of addresses in which to send letters.
- Have students draft a letter to the state representative of their choice.
- Have students exchange letters and offer feedback and constructive criticism.
- Have students rewrite their letters into final draft form based on suggestions for revisions.
- As a class, mail letters to the appropriate state representative.

Post-Assessment

Administer the post-assessment online at **www.isafe.org** by clicking on “Assessments” if this is your last lesson for i-SAFE. To verify school ID number, log in at **www.isafe.org**, go to the “My Info” page, and select “Find Your School ID.”

Related Lessons

The i-SAFE lessons: provide additional related information.

Contact us

We'd like to hear from you! E-mail **teachers@isafe.org** to share any unique ideas and/or experiences you had during implementation of this lesson.

Legal Trends – Cyber Bullying

Introduction

i-SAFE would love to be able to give you a set list of rules and say, "Follow these and you'll be always safe and secure." The problem is that it might ignore some of your rights when it comes to free speech, copyright, fair use, and what's more – it just won't accomplish anything. It also won't work to simply give you a set line and say, "As long as you only do this, you are OK." Those lines are still being drawn in the law books and courtrooms. It is important to remember that the Internet is still very young, and many of the issues that are coming up online are just now making their way to federal and state lawmakers, and courtrooms to decide. So let's talk about that! Think about the issues below, what the lawmakers are considering, your rights, and what you can do to get involved and influence final policy.

Cyber Bullying

Although youth have known about this issue awhile, it is just now coming to the attention of those who make the laws and policies because of some high-profile cases involving murders and/or suicides.

Schools are hurrying to develop school policies regarding cyber bullying that substantially disrupts class, is committed with school equipment, etc.

Federal lawmakers are targeting these issues with laws that encompass other issues like antistalking. One recent federal law makes it illegal to anonymously "annoy, abuse, threaten, or harass" another person over the Internet. However, many critics of such a law say that the wording is too vague and open to interpretation. How does one define what is "annoying," and when should a case be prosecuted? Other federal laws can cover some cases of cyber bullying in which direct threats are made, etc.

To make it even more confusing, various states are also enacting laws to cover the issue of cyber bullying.

Washington has pending legislation: State Sen. Jeanne Kohl-Welles sponsored a bill to end cyber bullying described as: "Harassment, intimidation, or bullying by any intentional electronic . . . act, when that act a) physically harms a student or damages a student's property; b) has the effect of substantially interfering with a student's education; c) is so severe, persistent, or pervasive that it creates an intimidating or threatening educational environment; or d) has the effect of substantially disrupting the orderly operation of the school.

Virginia has gone one step further with its legislation: People are guilty of "harassment by computer" if, intending to intimidate or harass they use a computer or network to "communicate obscene, vulgar, profane, lewd . . . or indecent language, or make a suggestion/proposal of an obscene nature, or threaten any illegal or immoral act." Harassment by computer is punishable by up to a year in jail or a substantial fine.

Think about it:

What are your state laws?

What are your school policies?

What types of laws would you like to see in place at various levels?

Legal Trends – Intellectual Property

Introduction:

i-SAFE would love to be able to give you a set list of rules and say, “Follow these and you’ll be always safe and secure.” The problem is that it might ignore some of your rights when it comes to free speech, copyright, fair use, and what’s more – it just won’t accomplish anything. It also won’t work to simply give you a set line and say, “As long as you only do this, you are OK.” Those lines are still being drawn in the law books and courtrooms. It is important to remember that the Internet is still very young, and many of the issues that are coming up online are just now making their way to federal and state lawmakers, and courtrooms to decide. So let’s talk about that! Think about the issues below, what the lawmakers are considering, your rights, and what you can do to get involved and influence final policy.

Intellectual Property:

Intellectual property and students is a VERY debated topic. There have long been fair-use guidelines covering what is appropriate for U.S. students to use in regard to education. However, the advent of the Internet has changed the whole playing field when it comes to copyright, piracy, fair use, and more.

The relative ease with which one can download material and use it has resulted in numerous court cases as the participants struggle to determine what the law should say. Are peer-to-peer networks legal? Do they have a valid purpose that is not illegal (i.e. downloading copyrighted music, movies, etc.) What about music? How should it be restricted when it comes to downloading, paying for play, use on computers and mp3 players, and more.

To understand many of the issues, it is important to note that intellectual property laws are designed NOT just to protect the creators of a work but also to protect public interests. For example, it is understood that for a creator to want to continue to produce work, there must be some type of ownership and monetary compensation in regard to value. Thus it is considered a person owns what they create and can sell the rights to the work. However, to encourage overall health of the creative community, it is also understood that items should eventually enter the public domain for free usage and that there are reasons for selective use that are valid, such as criticism, commentary, and more. These issues enter all new realms when the environment of the Internet is taken into consideration.

Think about it:

- According to 2005 statistics one in three music discs sold worldwide is an illegal copy
- How common is illegal downloading among your peers?
- Can you think of any effective solutions to illegal use of Intellectual property?

Legal Trends – Cyber Predation

Introduction:

At i-SAFE, we'd love to be able to give you a set list of rules and say, "Follow these and you'll be always safe and secure." The problem is that it might ignore some of your rights when it comes to free speech, copyright, fair use, and more. Nor can we simply give you a set line and say, "As long as you only do this, you are OK." Those lines are still being drawn in the law books and courtrooms. It is important to remember that the Internet is still very young, and many of the issues that are coming up online are just now making their way to federal and state lawmakers, and courtrooms to decide. So let's talk about that! Think about the issues below, what the lawmakers are considering, your rights, and what you can do to get involved and influence final policy.

Cyber Predation:

Unlike cyber bullying, for the most part, cyber predator laws are much more straightforward.

The first law targeting illegal predation acts and pornography on the Internet was the Communications Decency Act of 1996. This act attempted to regulate indecency in regard to children and also obscenity on the Internet. The Supreme Court struck down this act because it failed to take into account freedom of speech in regard to obscenity online.

In 1998, a comprehensive act passed through federal government called Protection of Children From Sexual Predators Act. The main target of this act was to set guidelines as they apply to interstate acts, such as solicitation or distribution across state boundaries, etc. This made it applicable to cases involving the Internet. This act encompassed several different components, including the following:

- It made it illegal to entice, engage, solicit, etc., for a child younger than 16.
- It made it illegal to distribute child pornography (such as over the Internet).
- It made it illegal to transfer to or target children younger than 16 with obscene material.
- It increased various penalties for various predator acts.
- It required Internet service providers (ISPs) to report actions that violate any of the above.
- Along with many other sections that help strengthen current laws, etc., it is designed to make it more difficult for cyber predators to operate and easier to prosecute said criminals and increase penalties and fines.

The story of Katie Tarbox may be familiar to you. It is the story of a 13-year-old girl who develops an online relationship with someone she believes is a 23-year-old named Mark. The online relationship results in her agreeing to meet with him at a hotel during a swim meet. When she arrives at his room, she discovers a 41-year-old pedophile named Frank Kufrovich. Luckily, the tryst was interrupted by her mother who was informed of the meeting by a friend of Katie's. This case became the first federally prosecuted case of this type resulting in a sentencing of only 18 months (despite evidence of this being a repeat offense and him having downloaded child porn on his computer). This case was prosecuted under the first act of 1996, and the following act of 1998 attempted to take into account sentencing and penalties.

Think about it:

- What types of penalties are adequate for online solicitation of minors?
- What types of penalties are adequate for child pornography?
- Should ISPs, Web site hosters, or peer-to-peer (P2P) software sites be responsible for material trafficked on their sites?
- How should the government pursue and track down such criminals?

Legal Trends – Malicious Code

Introduction

i-SAFE would love to be able to give you a set list of rules and say, "Follow these and you'll be always safe and secure." The problem is that it might ignore some of your rights when it comes to free speech, copyright, fair use, and what's more – it just won't accomplish anything. It also won't work to simply give you a set line and say, "As long as you only do this, you are OK." Those lines are still being drawn in the law books and courtrooms. It is important to remember that the Internet is still very young, and many of the issues that are coming up online are just now making their way to federal and state lawmakers, and courtrooms to decide. So let's talk about that! Think about the issues below, what the lawmakers are considering, your rights, and what you can do to get involved and influence final policy.

Malicious Code

While malicious code has been around for a long time, it has become more and more of an issue because of the large increase of the online population. As more and more people rely on and use high-speed electronic communications, e-mail attachments, and peer-to-peer file-sharing programs, viruses and worms will continue to spread.

The impact of viruses, worms, and Trojan horses is large-scale. It is economically debilitating and can run into the billions of dollars. There is the potential for homeland security risks and more. With these things to consider, causing damage to our nation's computer networks is a federal crime, one that carries substantial penalties for those convicted. The principal federal law-enforcement weapon in the battle against computer viruses and worms is the Computer Fraud and Abuse Act, 18 U.S.C. ' 1030.

The actual wording of the act is fairly broad. It states that the risk of damage from a computer virus or worm is significant and could impact critical national or personal interests. Penalties for felony violations of the law range from five to 20 years in prison for subsequent offenders, to life imprisonment for those whose knowing or reckless violations result in someone's death.

Unfortunately, because of the way the Internet was formed and the fact that computers are connected worldwide, laws in the United States do not necessarily apply to laws in other countries. Therefore, those who develop malicious code and release it in a different country may never be prosecuted. Their country may not have set laws for the crime, an adequate judicial system, etc. In addition, this leaves open an area of those in foreign countries who are condoned by their government for actions on foreign computers (i.e. terrorism or cyber warfare).

Think About It:

- Why, despite the harsh laws, do we not hear of more court cases and prosecutions in regards to malicious code?
- Is there a need for some type of international courtroom to handle Internet issues like malicious code? And if so, how would it work?

Get Involved in Changing Policies!

Write a letter to an elected official.

Materials/Preparation

- Decide which elected official you will write to. You can find out the names and addresses of your elected officials at <http://www.congress.org/congressorg/home/>.
- High-quality paper
- envelope and stamps

Brainstorm.

- Select the issue on which you will write, and gather information.
- Brainstorm your suggested policy solution.

Write the letter.

- Using the information you brainstormed, write your letter.
- Use the sample letter to a Congressman as a guide on how to format.

Edit.

- A letter to an elected official, such as a Congressman, should be carefully written, edited, and revised. Make sure to follow basic formal letter-writing standards. Clearly state the problem as you see it, and offer suggestions for ways of solving this problem through legislation or policy changes.
- Trade letters, and offer constructive criticism and feedback with other students.

Final Draft

- On high-quality paper, write your final draft.
- Seal letter in envelope, address, and mail.

Take it Further.

If you're seriously interested in helping form policy as an individual or as part of a club or class, i-SAFE can help you get it done! Contact outreach@isafe.org and/or visit X-BLOCK at <http://xblock.isafe.org/> for suggestions.

This is Moni, an i-SAFE student i-MENTOR from Maryland. This eighth-grader planned an entire Town Hall Event and an i-PARENT Program, and made sure the attorney general of Maryland had the SAFE Link on his Web site. He has been a speaker with i-SAFE to Congressional members at several Congressional briefings.



i-

You can do amazing things when you put your mind to it!

Sample letter to Congressional Representative

[Date]

U.S. Rep. _____

[See www.house.gov for addresses]

Washington, D.C. 20515

Dear [Mr./Ms.] _____:

1st paragraph: State who you are, the issue, why you are interested in issue.

Example: The purpose of this letter is to inform you of my concerns on . . .

2nd paragraph: Expand on issue.

3rd paragraph: Offer your suggestion for a solution.

4th paragraph: Conclude.

Sincerely,

[Name]

[Address]

[Telephone and/or e-mail]

LESSON—Learn Before You Burn

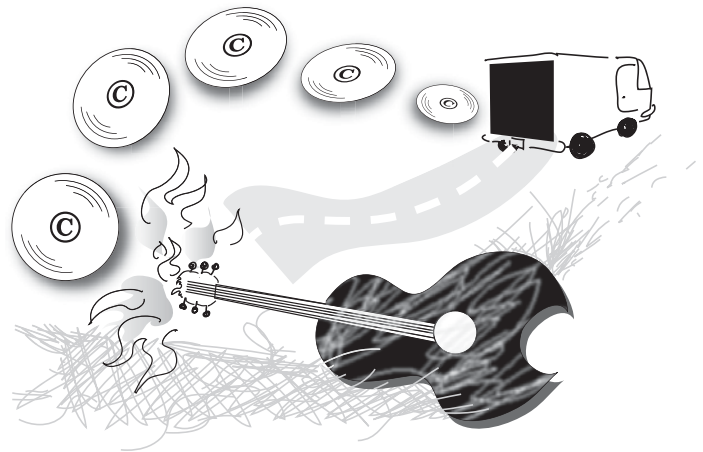
Unit: Music Rules: Learn Before You Burn

Supplement to the Music Rules: Learn B4 U Burn Assembly

Learning Objectives

Students will:

- be able to define piracy as it applies to the Internet, physical CDs, and burning for friends
- be able to differentiate between legal and illegal ways to acquire music
- identify legal resources for downloading music
- know the guidelines for use of music that is purchased legally
- understand the legal and personal consequences for illegally downloading and uploading music



Enrichment Goal

i-SAFE enrichment activities are designed to be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at <http://xblock.isafe.org>, including the i-MENTOR Training Network videos.

In this lesson, learners will develop public-service announcements (PSAs) to inform others about the risks of piracy and legal alternatives to the illegal downloading of music. The enrichment activity will provide guidance to broadcast one or more of the PSAs at school or through local news media.

Materials/Preparation

copies of the reference and activity pages for each student

Pre-Assessment

Prior to beginning the first lesson of the “Music Rules: Learn B4 U Burn” unit, please administer the pre-assessment online at www.isafe.org by clicking on “Surveys/Assessments,” entering the correct school ID number, pressing “Next,” and selecting “Illegal Music Downloading: Pre-Assessment” from the list of special assessments, which appears at the bottom of the next page. To verify school ID number, log in at www.isafe.org, go to the “My Info” page, and select “Find Your School ID.”

Lesson Procedures

All students participating in the i-SAFE curriculum are considered i-MENTORs. If they haven’t done so already, have students enroll online by clicking on “Create Account” at www.isafe.org to take full advantage of the support and incentives offered. This may be done at any time during the lessons, or students may complete this registration at home. If you would like to register your students yourself, simply go to <http://www.isafe.org>.

org/teachermentorprogram and fill out the information for your students; then e-mail to outreach@isafe.org. Your students will then be enrolled, will receive information about sharing Internet safety with other students, and will be registered to participate in contests to win prizes.

Discussion

Review with students the following information:

- Copyright is protection provided by the Constitution and laws of the United States to the creators of things like books or other written works, as well as other dramatic, musical, and artistic works. To be copyright protected, the works must be in tangible form.
- Copyrighted works are protected from being copied, distributed, performed, or changed without the creator's (or owner's) permission. This protection is available for both published and unpublished works, and applies to students' work. Illegal reproduction or unauthorized use of copyrighted work is often known as piracy.
- Intellectual property is copyright, patent, trademark, or other form of protection for material that is intangible (you can't touch it), including ideas, music, the written word, pictures. You may not be able to touch it, but it does have value and is often considered the property of the person who created it.

Survey Activity

- Pass out the survey activity to students.
- Have students complete the survey.

Survey Discussion

Pass out the "Piracy" reference page to each student. Instruct them to use the survey discussion to fill in the examples under each category of piracy.

Discuss the survey questions. Main discussion points are below.

1. I have illegally downloaded a song from the Internet.
 - Make the point that there are LEGAL ways to download music. Ask students what they might be.
 - Discuss illegal means of downloading music.
2. I have paid to download a song online.
 - Ask students who paid to download the music.
 - What types of sites allow the legal downloading of music? How do some of them work (pay a flat fee for a song, pay a subscription fee to listen to music, etc.)?
3. I have ripped CDs I own to MP3s and have made them available online for others via the Web or e-mail.
 - Ask students how they have used music they own online (on Web sites, for others to download, via e-mail attachments, etc.).
 - Is this legal? Why or why not?
4. I have used peer-to-peer (P2P) software to download music (or movies/software).
 - Review with students the dangers associated with peer-to-peer software: viruses, spyware, porn, legal issues, etc.
 - Can anyone give an example of a personal experience with any of these problems?

5. I have made a copy of a CD I own for someone else.

- Remind students that this is illegal.
- One can make a back-up copy or a personal mix of music for himself or herself but cannot give it to others.

6. I have knowingly obtained unauthorized music.

- Refer to the reference page, and read through the variations of music piracy.
- Discuss the various ways students can easily commit piracy without thinking of the consequences to others (i.e. receiving a shared MP3 from a friend, making a couple of copies of a CD and giving them to someone else, putting a favorite song on a personal Web site, etc.).

7. I understand how copyright protects items like music.

- Review with students why copyright laws exist (they protect the interests of creators).
- Ask: What could happen if we did not have copyright laws? Would creators/songwriters/singers, etc., still create?

8. I understand why there's a need for copyright laws.

- Discuss why students agree or disagree with copyright laws.
- What are some viable solutions to the arising copyright crisis?

Activity

Brainstorm as a class legal ways to download music, sites students have used, etc., and create a master list. Do an Internet search to find other examples.

Note: The Music United Website provides a comprehensive list of Websites where music can be downloaded legally. <http://www.musicunited.org/>

Enrichment Activity

Using what they have learned and the reference material resources, students work in small groups to develop public-service announcements (PSA) to inform others about the risks of piracy and great legal alternatives to the illegal downloading of music.

- Provide students with copies of the PSA activity reference page.
- Use the master list of legal ways to download music as a resource.
- Follow the steps outlined to create and produce a PSA.
- Present PSAs to the class for review.
- Broadcast PSAs.

Post-Assessment

If this is the last lesson to be completed in the “Music Rules: Learn B4 U Burn” unit, please administer the post-assessment online at www.isafe.org by clicking on “Surveys/Assessments,” entering the correct school ID number, pressing “Next,” and selecting “Illegal Music Downloading: Post-Assessment” from the list of special assessments, which appears at the bottom of the next page. To verify school ID number, log in at www.isafe.org, go to the “My Info” page, and select “Find Your School ID.”

SURVEY—Learn B4U Burn

1. I have illegally downloaded a song from the Internet.

Yes No Don't Know

2. I have paid to download a song online.

Yes No

3. I have ripped CDs I own to MP3s and have made them available online for others via the Web or e-mail.

Yes No

4. I have used peer-to-peer (P2P) software to download music (or movies/software).

Yes No

5. I have made a copy of a CD I own for someone else.

Yes No

6. I have knowingly obtained unauthorized music.

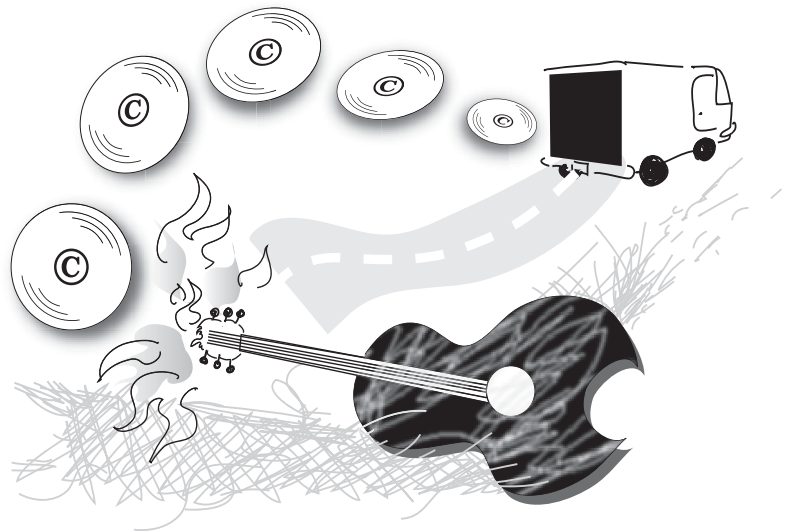
Yes No Don't Know

7. I understand how copyright protects items like music.

Yes No

8. I understand why there is a need for copyright laws.

Yes No Don't Know



ACTIVITY—Learn B4U Burn-Piracy

Directions

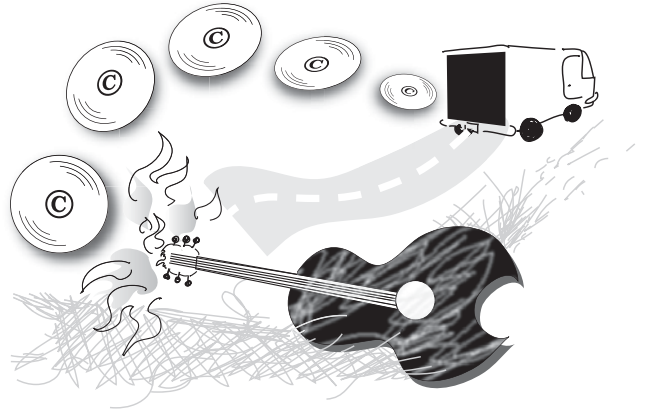
“Piracy” generally refers to the unauthorized reproduction and distribution of sound recordings.

Give an example of how each type of the following examples of piracy might occur.

Unauthorized CD Burning

This term refers to the unauthorized reproduction of a CD.

Example:



Online Piracy

This term is the unauthorized uploading and/or downloading of a copyrighted sound recording on an Internet site even if the recording isn't resold. Online piracy may now also include certain uses of “streaming” technologies from the Internet.

Example:

Counterfeit Recordings

These are unauthorized recordings of the prerecorded sound, as well as the unauthorized duplication of original artwork, label, trademark, and packaging.

Example:

Bootleg Recordings (or Underground Recordings)

These are the unauthorized recordings of live concerts or live musical broadcasts on radio or television.

Example:

Who's the Loser?

Illegal downloaders are the first to lose because the recording industry and law-enforcement officials are cracking down around the world. Do the crime, and you will pay a fine or do the time.

Consumers—that's you! Consumers lose because the work of pirates drives up the costs of legitimate products for everyone. Sometimes a consumer also unknowingly pays for a pirated tape or CD with inferior quality or defects. Pirated material can't be returned—it's a loss to the buyer.

Honest retailers and employees lose because they can't compete with the prices offered by illegal vendors. Less business means fewer jobs. These types of jobs are often filled by young people.

Record companies lose. Eighty-five to 90% of recordings released don't generate enough revenue to cover their costs. Record companies depend heavily on the profitable recordings to enable the less-profitable types of music to be produced.

Creative artists lose. Musicians, singers, songwriters, and producers don't get the royalties and fees they've earned. The cost of recording and promoting a major album can easily top \$1 million, and only one out of every 10 albums ever turns a profit. (MusicUnited.org)

Public Service Announcements - PSA

Grab people's attention and educate them at the same time!

Your Goal

Explore the issues involved with Internet piracy and develop a public service announcement to educate others about the risks of, and legal alternatives to, illegal downloading.

The PSA can be audio, video, or live. Part of the project is locating a broadcast medium.

Materials/Preparation

- Background knowledge on copyright and music piracy issues
- Computer with Internet access (recommended)
- Materials of choice for developing PSA (video, audio, etc.)
- Obtain cooperation with school media outlet, radio, TV, or other broadcast medium

Issues

Take a minute and think about the following before you decide how to present your information.

- How can PSAs about music downloading be of service to others?
- What information do you consider "critical" when it comes to information about digital music use.
- Who is this information "critical" for?
- How can you grab people's attention and make them listen to your important message?
- Based on what you know about piracy, what information will be most beneficial?

Preparation

1. Go to www.isafe.org and review the celebrity PSAs
2. Find a Media Outlet – will it be at your school or in the larger community?
3. Brainstorm—where can PSAs be played in your school or in your city?
 - Some possibilities: over the school PA system, at assemblies, over the radio, on a local news station, over the PA at a baseball game. What new ones can you come up with?
4. If going outside of the school, contact the media outlets to develop a cooperative agreement for broadcasting the PSAs.
 - Contact the media outlet before preparing your PSA to get their specific requirements regarding length, format, etc.

Develop and Deliver PSA

1. Based upon media outlet—select media type—audio, video, or live
2. Write the script that pertains to your topic and presentation style (i.e. audio, video, etc.)
3. Record the PSA (unless doing it live)
4. **Don't forget music!** Edit the PSA with original music and titles – you'll be demonstrating legal music use! (i-SAFE provides a free library of legal music and graphics at www.isafe.org.)
5. Provide PSA through the selected media outlet.
6. Let i-SAFE know about your success. Email outreach@isafe.org.



www.isafe.org

~ Send a copy of your own PSA to i-SAFE so we can hear about your creativity. Your PSA may be used in future T-Kits! ~

Cyber Relationships

Webcast Lesson Plan

i-SAFE Lesson Plan

Suggested Grade Level – High School

Video Access Options

This video Webcast is available at no cost for streaming via www.isafe.org. See instructions on page 2 under “Access the Webcast”.

The Webcast may also be purchased on DVD at <http://auth.isafe.org/store/>.

Description

This webcast is designed to raise student awareness to the risks they face while communicating online. It addresses harassment, cyber stalking, and the process of *grooming*, used by cyber predators to prepare their intended victims for face-to-face meeting. The primary objective of this lesson is to educate and empower students with knowledge that will enable them to assertively protect themselves while communicating online to decrease the chance that they will be victimized online.

The lesson is comprised of several key elements:

- 1) The webcast delivered via www.isafe.org (click on quick link *webcasts*)
- 2) Three directed discussion breaks during the webcast for the students in the classroom, facilitated by the classroom instructors
- 3) Cooperative group exercises at the conclusion of the webcast
- 4) Pre- or post-assessment if this is either the first or last lesson in your i-SAFE program. Click on the link: Assessments at www.isafe.org

Learning Objectives

Students will:

- understand how to communicate more safely online with proactive techniques
- understand how to refuse requests for information, unwanted solicitations, and requests to participate in unlawful online activities
- know how to report suspicious, unlawful, dangerous, or threatening online behavior and activities
- develop a strategy to inform others about how to protect themselves while communicating online

Enrichment Goal

i-SAFE enrichment activities are designed so that they can be implemented by students.

Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at www.isafe.org.

In this lesson, learners will interact in the classroom environment through group discussion and examination of online privacy issues. Learners will be provided with materials to engage in an enrichment activity, which includes which includes using i-SAFE materials to host a student assembly on Internet safety issues.

Materials / Preparation

- Access to the Webcast, *Cyber Relationships*
- A copy of the Enrichment Activity pages: Hosting the i-SAFE Assembly Experience
- Online i-Mentor registration (each student) to receive supporting online training videos and Student Toolkit materials

Pre Assessment

If beginning the i-SAFE program with this lesson, administer the pre assessment online at www.isafe.org by clicking on the link, Assessments, prior to the lesson. To verify School ID#, login at www.isafe.org, go to the "My Info" page and select "Find your school ID".

Lesson Procedures

All students participating in the i-SAFE curriculum are considered to be mentors. If they haven't done so already, have students enroll online by clicking on "Create Account" at www.isafe.org to take full advantage of the support and incentives offered. This may be done at any time during the lessons, or students may complete this registration at home. If you would like to register your students yourself simply go to <http://www.isafe.org/teachermentorprogram> and fill out the information for your students and email to outreach@isafe.org. Your students will then be enrolled to receive information about sharing internet safety with other students and registered to participate in contests to win prizes.

Access the Webcast

Access the webcast at www.isafe.org by clicking on quick link Webcasts. To find School ID Number: Login and check your "my info" page at www.isafe.org for school id #.

A high-speed Internet connection (T1, ISDN, DSL or Cable Modem) is needed to view the Webcast. If you do not have a computer with a high-speed Internet connection, this Webcast may be purchased on DVD at <http://auth.isafe.org/store/>.

Activity 1

This is a short activity, approximately 2 minutes in duration.

Ask your students think about incidents they know about concerning a victim of sexual solicitation, online grooming, harassment, or cyber stalking.

Play the web cast; pause at the first discussion break.

Synopsis of Web Cast – Part I

Maribel and Rafael discuss the risks of using the Internet and Carla introduces the *grooming process*.

Discussion 1

This is the first discussion break in the web cast. Lead the students in a discussion about the grooming process and write their responses on the board.

To prepare the students to answer Question #1, ask them the following:

- Carla just introduced the term *grooming process*. Do you remember the definition?
Answer: The process used by a cyber predator to win the victim over and prepare them for a face-to-face meeting.
- Raise your hand if you have ever had a conversation online with someone you did not know.

-
- Have the students *think* about the following:
 - Have you ever thought the person you were talking with online was not telling the truth about themselves? What made you suspicious of them?
 - When you have felt comfortable with the person you are talking with online, what did they say that made you feel safe?
 - Do you think a cyber predator would want you to feel suspicious or safe while you are talking to them?

Question – What does the term *grooming* as it relates to cyber predators mean?

Definition: The process used by predators to gain the trust of victims and to build false relationships.

The steps of the grooming process are presented in the next section of the web cast. The purpose of this exercise is to get the students to start thinking about conversations they have had online, to recognize, as per the definition of the grooming process, that a cyber predator will initially try to create an amiable relationship with them, and that the goal of the predator is to have a face-to-face meeting with them.

Synopsis of Web Cast – Part II

Carla presents the steps of the grooming process. Then an example of a private chat room conversation between Boardude22 and SexyCindy14 is presented to illustrate what to avoid saying or what to look for, in order to avoid being groomed, harassed or cyber stalked.

Discussion 2

Lead the students in a discussion about online situations they have encountered in which online they have given out personal information, and how they can protect themselves from revealing too much personal information. Write their responses on the board for each of the following question.

Question – What are some of the things Cindy could have done which might have been safer? If students have a difficult time recalling Cindy's conversation, ask them the following questions:

Q. What was Cindy's screen name?

A. SexyCindy14

Q. What does that reveal about Cindy?

A. Her name, gender, and that she is probably 14 years old.

Q. Where does Cindy go to school?

A. Adams High School

Q. Was there anything suspicious about Boardude22's responses?

A. He became very angry with Cindy

The goal is to help the students to come to the conclusion that Cindy has put herself in a potentially dangerous situation, as "Boardude22" now knows her name, her age, where she goes to school, and possibly her phone number. It is also likely that in a previous conversation Cindy may have revealed other identifying information. Predators tend to piece together information over a series of conversations and create profiles. Students need to realize that giving out what may seem like innocent information could lead to the creation of a very descriptive profile that a predator could use to find them.

Synopsis of Web Cast – Part III

Carla gives tips on how to be safe while communicating online. Then online harassment is defined, and statistics pertaining to online harassment are presented.

Discussion 3

Lead the students in a discussion about online harassment.

Question #1: When does online behavior become online harassment?

To help the students answer this question, you might want to ask them for the following:
What is online harassment?

Answer: Any message that is abusive, sexually explicit, violent, encourages dangerous or illegal activities or is just annoying.

Question #2: How does online harassment make one feel? (Annoyed, angered, frightened.)

The purpose of this question is to illustrate that there are varying degrees of harassment and a variety of responses.

Question #3: What should you do if you are harassed online?

The purpose of this exercise is to get the students to recognize when they are being harassed, what to do at the moment they realize they are being harassed, and that it is imperative that they report the harassment if they feel threatened or annoyed.

Synopsis of Web Cast – Part IV

Maribel and Rafael discuss what to do if you are harassed. Then Detective Chris Hicks of the Los Angeles Sheriff's Departments discusses the differences between harassment and cyber stalking. Detective Hicks ends the discussion with tips on what to do if you think you are being harassed or stalked.

Activity

In this class activity, have your students break into groups for a cooperative learning activity. Have each group select a spokesperson to relate the results of their discussion to the rest of the class.

1. Ask the students to individually recall and write down the key steps in the grooming process.
2. Ask the students to share their answers with their group.
3. Ask each group to use the key steps and techniques of the grooming process to create what they believe would be a typical private chat or instant messaging conversation between a cyber predator and his or her victim.
4. Have each group share their conversation with the class. At the end of each presentation have the class identify the steps and techniques of the grooming process that were used in the conversation.

Discussion 4

Use the examples created by the students to stress the importance of protecting themselves online. Explain that if they think they are being groomed or cyber stalked, they need to report these actions. Discuss the various reporting systems available to them if they believe they have been victimized online. Options include the following:

Report in person to:

-
- Local police
 - Teacher or other adult at school (you may want to provide specific information on who to contact at the school based on school policies)

Report by phone:

- Local police (provide the phone number)
- FBI (provide the local phone number)
- Crime Stoppers (provide the local phone number)

Report by phone or online:

- Your Internet Service Provider (ISP)
- CyberTipline (www.cybertipline.com)

The National Center for Missing and Exploited Children (NCMEC) has a system for children to report incidents when they receive “messages or images that are obscene, lewd, filthy, or indecent with the intent to harass, abuse, annoy, or threaten” them. NCMEC recommends that children report the incident to the Internet Service Provider and the CyberTipline (www.cybertipline.com) or by calling 1-800-843-5678.

Conclusion

- Lead into a discussion about the Enrichment Activity.
- Provide a copy of the page: *Assembly Experience* to each student.
- Discuss why it is important for older students to share what they know about Internet safety.

Enrichment Activity

Youth who participate in activities to share what they have learned about Internet safety are more likely to practice safe habits online. Additional lessons and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. www.isafe.org.

i-SAFE provides the easy to access i-Mentor Training Network videos at no cost to help students share their knowledge about Internet safety with the uninformed. The 8-10 minute videos provide specific “how to” information on accomplishing i-SAFE outreach activities. They are available to students by going to the X-Block at www.isafe.org and selecting the i-Mentor Training Network.

The enrichment activity for this lesson is the *Assembly Experience*, designed to provide materials and training to help older students put on an assembly about cyber predators. Students can put on the assembly at your school or at a middle school.

Student Instructions:

Registration

- Go to www.isafe.org and register
- Access to the i-Mentor Training Network, Module: Assembly Experience
- Complete the module and download the i-SAFE Student Toolkit
- Follow the online instructions to receive your Assembly Experience: What’s the Download CD/DVD set

Materials/Preparation

- DVD player

-
- i-SAFE Assembly Experience CD/DVD set
 - Additional i-SAFE Assembly Experience materials detailed on the CD
 - Print copies of the *Student Toolkit* from the Curriculum CD
 - Permission of school to host assembly

Preparation

View the PowerPoint® “How to Host an Assembly” for background information on hosting a school assembly and detailed information on the materials i-SAFE provides.

Develop the Assembly

Follow the instructions in the PowerPoint and the i-Mentor Training video to put together your assembly.

Be sure to give time for designing items, requesting speakers, etc.

Request permission for use of the school gym, auditorium, etc. at the middle or high school of your choice.

Host the Assembly

Host your school assembly. Take photos, and document the event.

Let i-SAFE Know!

Contact outreach@isafe.org with details of your assembly. Students may be eligible for i-SAFE's most valuable mentor award.

Post Assessment

Administer the post assessment online at www.isafe.org by clicking on the link, Assessments, if this is your last lesson for i-SAFE. To verify School ID#, login at www.isafe.org, go to the “My Info” page and select “Find your school ID”.

Related Lessons

The i-SAFE lessons: Identity Theft, and Online Shopping provide additional related information.

Contact us

We'd like to hear from you! E-mail teachers@isafe.org to share any unique ideas and/or experiences you had during implementation of this lesson.

i-SAFE Internet Life Skills Preview

Series 2 Workbook



In today's world, many life skills tasks, from bill paying to applying for a job, are accomplished via the Internet. Before taking advantage of the many opportunities the Internet provides, it is important to know how to maintain personal safety and computer security while engaging in these tasks. This lesson provides a preview of the lesson activities provided in the complete Internet Life Skills Series 2, available for purchase from i-SAFE at <http://auth.isafe.org/store/>

Complete Workbook Overview

Internet Life Skill Series 2

- Your Online Persona (covers personal Web site and profiles)
- Online Social Networking
- Online Relationships
- Multi-user Online Gaming
- Peer-to-Peer Networking

Understanding the Workbook

This Internet Life Skills series workbook is designed to help you master a selection of basic online life skills. Each lesson is presented in sections to fully address the topic. Lesson sections include:

- **Topic Overview:** General description of the topic
- **Vocabulary:** Critical terms and definitions used in the lesson
- **Talk About It:** Provides thought provoking questions. Depending on classroom set-up students can be directed to discuss with a partner, in a small group, or as a class.
- **Free Write:** Supports exploration of the topic through a writing prompt and space to jot down thoughts and previous knowledge.
- **Think About It:** Reference information and materials to consider specific to the topic.
- **Activity:** Each activity section includes directions to complete either a directed or worksheet activity to support learning.
- **Go Online:** This section provides an activity set up by the instructor to go online and apply what has been learned, either by researching a topic or completing a task.
- **Reaching Others:** This section provides guidance for extending what has been learned by sharing this information with others.



Additional Resources

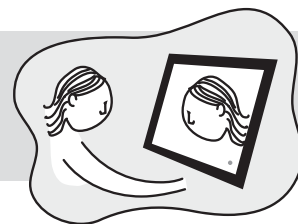
Your instructor may provide you with additional online and/or offline resources to complete these lessons.

Completion Quiz

Your instructor may administer a series quiz upon completion of the workbook.

Your Online Persona

(Section 3 of the complete lesson)



Topic Overview

Using the Internet for any activity opens up the user to a variety of security risks including risks to the computer and threats to personal security.

The complete lesson covers four main areas of online personal safety and security maintenance:

1. e-mail address
2. screen name / user ID
3. password
4. personal Web site

Goal: The goal is for you to (a) understand the importance of online safety and security measures that allow you to maintain your personal safety and security while maintaining an online persona, and (b) to know how to implement those safety and security measures.

Section 3 of the complete lesson covers Personal Web Sites and includes the following:

Think About It

Personal Web sites have become very popular and a great way of sharing with family and friends. However, many people forget that other people can see the same Web sites.

One of the best options for protecting yourself, your site, and your personal information is to password protect your Web site. Only give the password to those you want viewing your site. This can eliminate many of the hazards of owning a personal Web site.

However, if you don't choose to password protect your site—take some precautions to protect yourself and your identity. Remember—anyone who does a Web search on you can find your site—this includes future employers, potential dates, and more.

See the tips below:

To be safe, AVOID the following:	DO take these Precautions
The use of your real name in your e-mail address	If you post an e-mail address, make sure it is anonymous (that does not contain identifying information)
The use of your real name on your site	Make up a nickname and stick to it when posting
Posting personal information on your Web page like phone number, address, birth date, etc.	Keep postings fairly anonymous
Posting pictures	If you must have pictures on your site, password protect the entire site so that only those you allow can gain access
Blogging about your personal life	If you must have pictures on your site, password protect the entire site so that only those you allow can gain access
The use of a Webcam or streaming video	Limit webcam use to family calls or interactions with personal friends, not for the public to view
Posting your IM screen name or giving it out to strangers	Give your IM screen name only to those you know from the physical world
Posting your IM screen name or giving it out to strangers	Give your IM screen name only to those you know from the physical world

Go Online



Take some time to research ways personal Web sites can be hosted. List the pros and cons of the various Web hosting sites you find.

PROS

CONS



Web Site Password Protection

Perhaps the easiest way to add password protection to your Web site is by using a free online service. All you have to do is sign up and add some code to your homepage. Most of them work by simply giving you a code to add to your HTML after you sign up with them. This code creates a box for your readers to enter their username and password so they can get to your password protected pages.

One security feature this enables is that when a viewer is brought to the page they will never see the direct URL at the top in the address line. They will only see the link box URL. This way they can never get to the page directly and will always have to go through your homepage to get there. If you ever decide you don't want a certain person to be able to access the page anymore you can block him or her by changing the password. You can then give the new password to everyone else (and not the person you want blocked). The downside to this type of password protection is that if someone somehow does get hold of the direct URL of the page they will still be able to access it.

Go Online (optional)



For more information and options for sites that will provide free password protection code, use your favorite search engine to search a phrase such as *download free Web site password protection*.

Or

Go to the list of sites provided by your teacher.



Self check

Complete the following "self-checks" relevant to the Web search concepts presented in this lesson.

- ☐ I understand how to develop a personal Web site that is safe and secure.

Reaching others



Home

Consider revising your personal screen name, password, profiles, Web sites, etc. Use the tips you've learned to ensure that you never reveal personal information when online to keep yourself safe and secure.



Community

i-SAFE provides a variety of programs to reach others with Internet safety awareness and education. Are you in a position to provide community service by teaching youth, parents or community members about Internet safety? Go to www.isafe.org to learn more educator, youth, parent, and community programs.

Service Learning: i-ADOPT-A-SCHOOL

i-SAFE LESSON PLAN

Goal

Using i-SAFE resources, learners will share what they have learned about Internet safety with their peers, family, and/or larger community.

Materials/Preparation

- i-SAFE Webcast DVD and player
- Computer with Internet access (recommended)
- Print copies of the Sharing Internet Safety handout and the *Student Toolkit*
- Coordinating i-SAFE materials (Lesson Plans, *i-Buddy Times*)
- Cooperation with younger class, club, or after school program

Lesson Procedures

Introduction

Introduce students to the concept of Service Learning—Aiding others in their community while learning and internalizing lessons. Instruct students that they will be learning about Intellectual property by viewing a Webcast, reading a lesson plan written for younger students, and viewing an *i-Buddy Times*. They will then use these materials to instruct others.

Registration

1. Go to www.isafe.org and register by clicking on "Create an Account"
2. Access the i-Mentor Training Network, Module: i-Adopt-A-School
3. Complete the module and download materials
4. Submit an online IP to receive i-SAFE curriculum materials (select *Classroom Instruction*) for the selected grade level of the child or children you are going to teach.

Background Information (Example provided - choose any Internet safety topic)

1. View the Webcast *Intellectual Property*.
2. Read either Grade 3 or Grade 4 Intellectual Property Lesson.
3. View the *i-Buddy Times* on intellectual property (found on the pages following this section).

Preparation

1. Research and find a targeted audience
 - Brainstorm—where can you teach younger kids about intellectual property?
 - Some possibilities: local elementary schools, after school clubs, boys or girls club, local library. What can you think up?
2. Contact your options about teaching a lesson on intellectual property.
 - Set up a firm date and time.
 - Be prepared on your topic so you can “sell” them on the idea over the phone. (i.e. the benefits, why it is necessary, how you are trained, etc.)

Teach a Lesson

1. Arrive early at your location and get set up to teach.
2. Make sure you have any copies or materials you need to teach.

-
3. Follow the lesson plan for either Grade Three or Four.
 4. Use the *i-Buddy Times* (on the following pages) as a supplement to the lesson.

Conclusion

Submit documentation to i-SAFE on completed lesson. Email to outreach@isafe.org

Option for Other Grades

Follow the lesson plan as above but make the following adjustments:

1. If the targeted audience is younger or older than grades 3-4, have Service Learning students select a Webcast topic they are interested in:
 - Privacy and the Internet
 - Cyber Relationships
 - Intellectual Property
 - Security: Malicious Code
 - Security: Cyber Citizenship
 - Cyber Bullying
2. Submit an online IP to receive i-SAFE curriculum materials (select *Classroom Instruction*) for the selected grade.
3. Select an i-SAFE lesson to implement in the class or after school program.
4. Review selected lesson with Service Learning students and make preparations to teach younger students.

Sharing Internet Safety Education

Educate younger students about Internet safety issues

You can teach students about Internet safety one-on-one or in a group setting. i-SAFE provides the easy to access i-Mentor Training Network videos at no cost to help YOU share your knowledge about Internet safety with the uninformed. The 8-10 minute videos provide specific “how to” information on accomplishing i-SAFE outreach activities. They are available by going to the X-Block at www.isafe.org and selecting the i-Mentor Training Network.

Get Started

1. Go to www.isafe.org and register
2. Access to the i-Mentor Training Network, Module: i-Adopt-A-School
3. Complete the module and download the i-SAFE Student Toolkit

Prepare

1. Brainstorm—where can you teach younger kids about Internet Safety?
 - Some possibilities: local elementary schools, after school clubs, boys or girls club, local library. What can you think of?
 - It doesn't have to be at a school - You can even teach and mentor 1 or 2 younger children – your siblings or children you babysit.
2. If you are going to teach at a school or club, make contact with an appropriate person about teaching a lesson on internet safety.
 - Set up a firm date and time.
 - Be prepared on your topic so you can “sell” them on the idea over the phone. (i.e. the benefits, why it is necessary, how you are trained, etc.
3. Submit an online IP to receive i-SAFE curriculum materials (select *Classroom Instruction*) for the selected grade level of the child or children you are going to teach.

Teach – be a mentor!

Teach a group lesson

1. Arrive early at your location and get set up.
2. Make sure you have any copies or materials you need to teach.
3. Contact outreach@isafe.org if you have any questions about teaching the lesson.

OR

Teach an informal lesson

For teaching less formally, such as one-on-one, gather your material such as activity pages – maybe you will want to combine safety instruction with knowledge about general computer use. Have fun!

